DEFENSE INFORMATION SYSTEMS AGENCY

DEFENSE RED SWITCH NETWORK (DRSN) OPERATIONS AND MAINTENANCE (O&M) GUIDE

APRIL 2001

TABLE OF CONTENTS

PART I
DRSN OVERVIEW

SECTION **PAGE**

SECTION **PAGE**

PART II
SITE ADMINISTRATION PROCEDURES

SECTION **PAGE**

PART III
SITE O&M PROCEDURES

SECTION **PAGE**

LIST OF FIGURES

LIST OF TABLES

TABLE **PAGE**

SECTION 1
INTRODUCTION

1.1 PURPOSE

The purpose of the *Defense RED Switched Network (DRSN) Operations and Maintenance (O&M) Guide* is to provide a comprehensive and concise overview of policies and procedures related to the operations, maintenance, and network management (NM) of the DRSN. This guide is intended to facilitate operations, maintenance, and management of the network and to foster network quality and cohesiveness through network wide standardized practices. The guide is not intended to replace referenced directives, but rather to provide a quick reference source for O&M personnel involved in the day-to-day DRSN O&M activities. To obtain a software copy of this guide, log on to the DRSN Electronic Bulletin Board System (EBBS). To access the EBBS, follow the methods as described in Section 9.4 of this guide.

1.2 GOALS AND OBJECTIVES

The goal of this guide is to provide the O&M personnel with a user-friendly, reference document for the day-to-day O&M procedures.

The main objective of this guide is to provide the DRSN site technician with a living document, a useful and practical tool for continually improving the quality of the DRSN to effectively provide uninterrupted service to all users of the network.

1.3 ORGANIZATION

This guide contains three parts: DRSN Overview, Site Administration Procedures, and Site O&M Procedures.

a. Part I: DRSN Overview. Part I, which begins with Section 3, provides a brief overview of the DRSN and DRSN subsystems, including switching, transmission, timing and synchronization (T&S), and NM.

b. Part II: Site Administration Procedures. Part II (begins with Section 5) addresses the DRSN administrative processes of site NM (data collection), security management, ordering telecommunications service, and record keeping (site configuration, maintenance, and inventory).

c. Part III: Site O&M Procedures. Part III (begins with Section 10) covers the day-to-day DRSN O&M procedures for fault management (FM), status reporting, preventive maintenance, and logistics (repair parts) support.

1.4 DEVELOPMENT

The *Defense RED Switched Network* (*DRSN) Operations and Maintenance (O&M) Guide* should be viewed as a living document that will continually change and improve. The users of the guide are invited to provide ideas and suggestions to enhance the guide, as it is field tested over time. DRSN O&M personnel may send comments and input for the guide to the following address:

DISA/NS541
ATTN: Jim Seitz
11440 Isaac Newton Square
Reston, VA 20190-5006

E-Mail Address: seitzj@ncr.disa.mil

DSN: 653-8032
Commercial: (703) 735-8032
FAX: (703) 735-8980

SECTION 2
DRSN DOCUMENTATION

2.1 OPERATIONS AND MAINTENANCE SITE REQUIRED AND RECOMMENDED DOCUMENTS

Table 2-1 is a list of required and recommended documents for all DRSN O&M sites. Documents marked with one asterisk "*" are recommended. Two asterisks "**" indicate required documents.

Table 2-1. O&M Site Required and Recommended Documents

DOCUMENT NO.	PUBLICATION TITLE
DISAC 300-85-1*	*Reporting of DCS Facility & Link Data*, 6 April 1993
Joint Staff Memorandum J-6A 016650-92*	*Operational Requirements Document (ORD) for Secure Voice Requirements*, 17 November 1992
DISAC 310-70-1**	*Defense Information Infrastructure (DII) Technical Control*, 25 June 1998
DISAC 300-115-7**	*Defense RED Switch Network (DRSN) Security Guide*, November 1995 (currently under revision)
DCID 1/21*	*Physical Security Standards for Construction of Sensitive Compartmented Information Facilities*, 30 January 1994
DIA Manual 50-4*	*Security of Compartmented Computer Operations*, 24 June 1980
DODD 5210.73*	*Security of DOD Communications Facilities*, 30 April 1984
DISAC 310-90-1*	*Physical Security Measures for DCS Facilities*, 10 November 1983
DISAC 310-130-1**	*Submission of Telecommunication Service Requests (TSRs)*, 4 April 2000
CJCSI 6215.01*	*Policy for the Defense Switched Network*, 1 February 1995
TM 97-008-OM Raytheon, E-Systems**	*Raytheon DSS-1 O&M Interactive Electronic Technical Manual*
DISAC 310-55-1**	*Status Reporting*, 21 January 2000
DISAC 310-70-84**	*Defense RED Switched Network (DRSN) Network Management Guide*, August 1994 (currently under revision)
AR 700-129/OPNAVINST 4105.2A/AFR 800-433/MCO 4110.2 **	*Joint Logistic Support Plan (SP) for DRSN*, 13 July 1998
DISAN 210-0-1*	*DISA Circulars and Notices*, 10 February 1998
DISAC 220-15-1*	*DISA Area Outstanding DII Facility Awards*, 8 April 1998
DISAC 300-175-9*	*DII Operating-Maintenance Electrical Performance Standards*, 8 June 1998
DISAC 310-70-1, VII, Sup I**	*DII Technical Control Test Description, Volume II, Supplement 1 Procedures Test Descriptions*, 8 May 1998
DISAC 310-70-86**	*DRSN Configuration Management Guide*, August 2000 (Final Draft)

2.2 DISA PUBLICATION ORDERING

To order DISA publications that are classified or not available on the DISA Web site, use the following steps:

1. Locate required publication in DISA Notice 210-0-1, *Index: DISA Circulars and Notices*
2. Complete DISA Form 117 (E)
3. Mail request order to:

DISA Publications Office
c/o DISA/CIO
701 South Courthouse Road
Arlington, VA 22204-2199

4. Fax request order to:

DSN Fax: 653-1977
Commercial Fax: (703) 696-1977
Attn: Publications Office

(703) 607-1890

PART I.
DRSN OVERVIEW

DRSN SUBSYSTEMS

- General
- Switching Subsystem
- Transmission Subsystem
- Timing and Synchronization Subsystem
- Network Management Subsystem

DRSN NETWORK MANAGEMENT

- General
- Network Management Subsystem
- Fault Management
- Performance Management
- Configuration Management
- Accounting management
- Security Management
- Network Management Responsibilities
- Network Management Point of Contact

Intentionally Left Blank

SECTION 3
DRSN SUBSYSTEMS

3-1. GENERAL

The DRSN, an element of the Defense Information Systems Network (DISN), is a network of secure command and control switches that provide high-quality secure voice and conferencing capabilities to the senior decision makers and staff of the National Command Authorities (NCA), the Commanders in Chief (CINCs), Major Commands (MAJCOMs), other Government departments and agencies, and Allies.

The mission of the DRSN is to provide the ability to transfer voice and data between the NCA, the National Military Command Center (NMCC), combatant commands, the Services, subordinate organizations (military and civilian), and Allies (North Atlantic Treaty Organization (NATO), Canada, etc.), both locally and worldwide. The DRSN also provides secure voice conferencing and access to secure strategic, tactical, airborne, and sea borne equipment and platforms.

The DRSN consists of four major subsystems: (1) Switching Subsystem, (2) Transmission Subsystem, (3) Transmission and Switching (T&S) Subsystem, and (4) Network Management Subsystem (NMS). The subsystem descriptions are intended to provide the reader with a general understanding of the DRSN. Figures 3-1 and 3-2 illustrate the current DRSN topology. See the Defense RED Switch Network (DRSN) Interface Criteria for more detailed descriptions of each subsystem and its respective component equipment.

3.1.1. Switching Subsystem

The DRSN Switching Subsystem provides the DRSN users secure and nonsecure call origination and call termination capabilities, secure conferencing, and direct interoperability with other secure networks. The primary switching platform of the DRSN Switching Subsystem is the Raytheon family of secure digital switches (SDS). In most DRSN switch locations, both a RED switch and a BLACK switch are installed to provide integrated RED/BLACK service (i.e., users are provided a single telephone instrument with which they can access both secure networks and nonsecure networks). A notional overview of a DRSN node is shown in Figure 3-3.

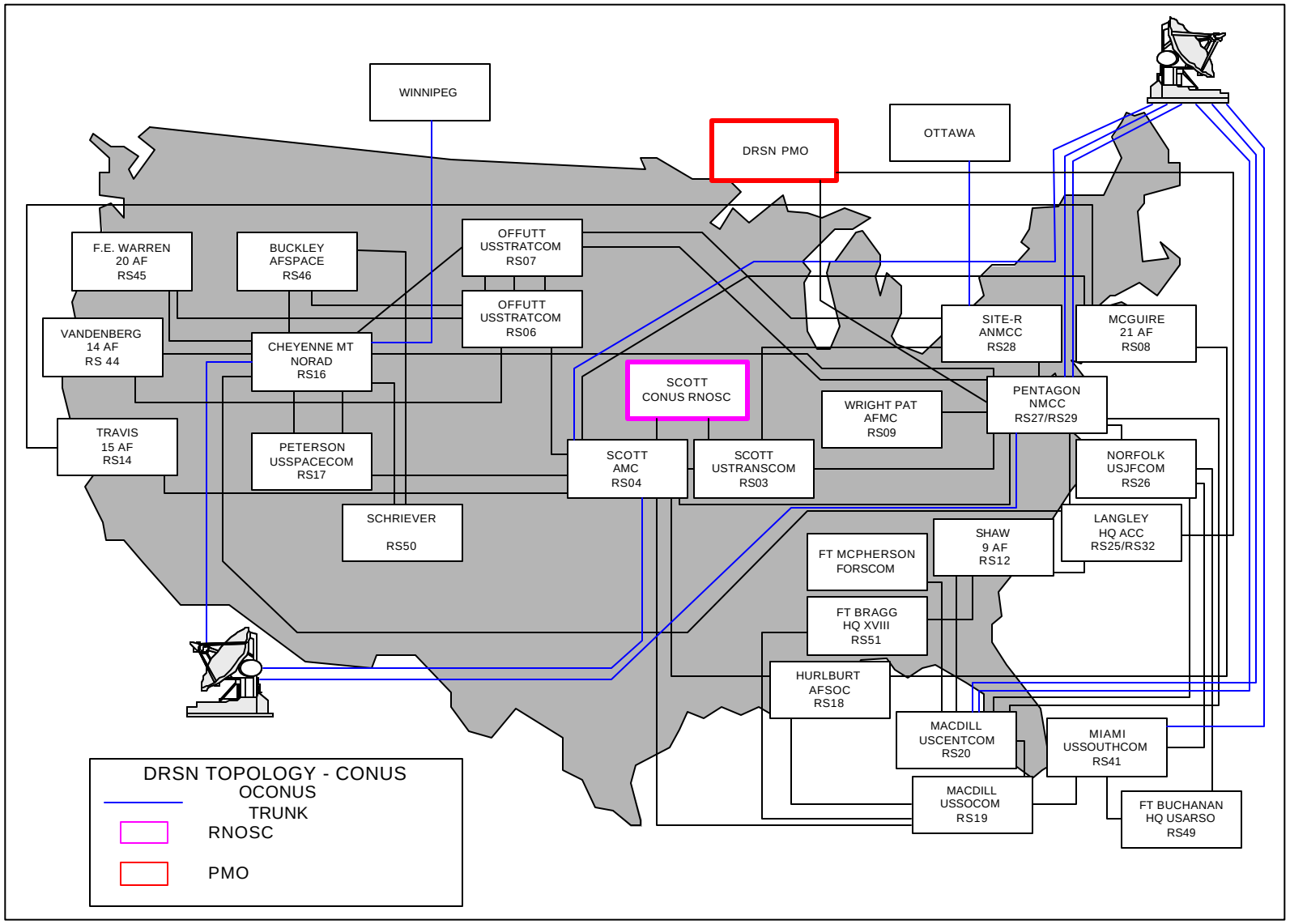

Figure 3-1. DRSN CONUS Topology

FOR OFFICIAL USE ONLY

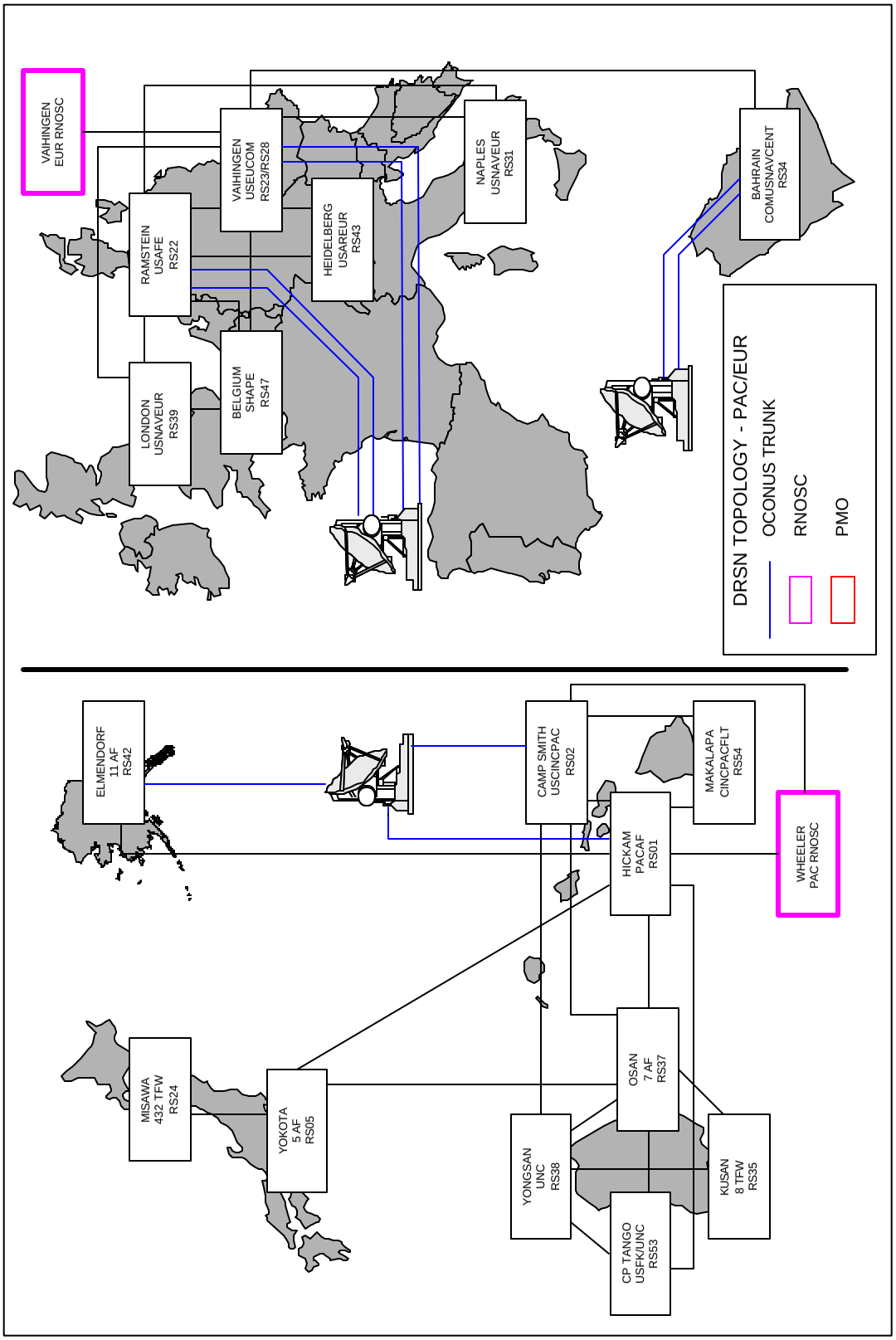

Figure 3-2. DRSN OCONUS Topology

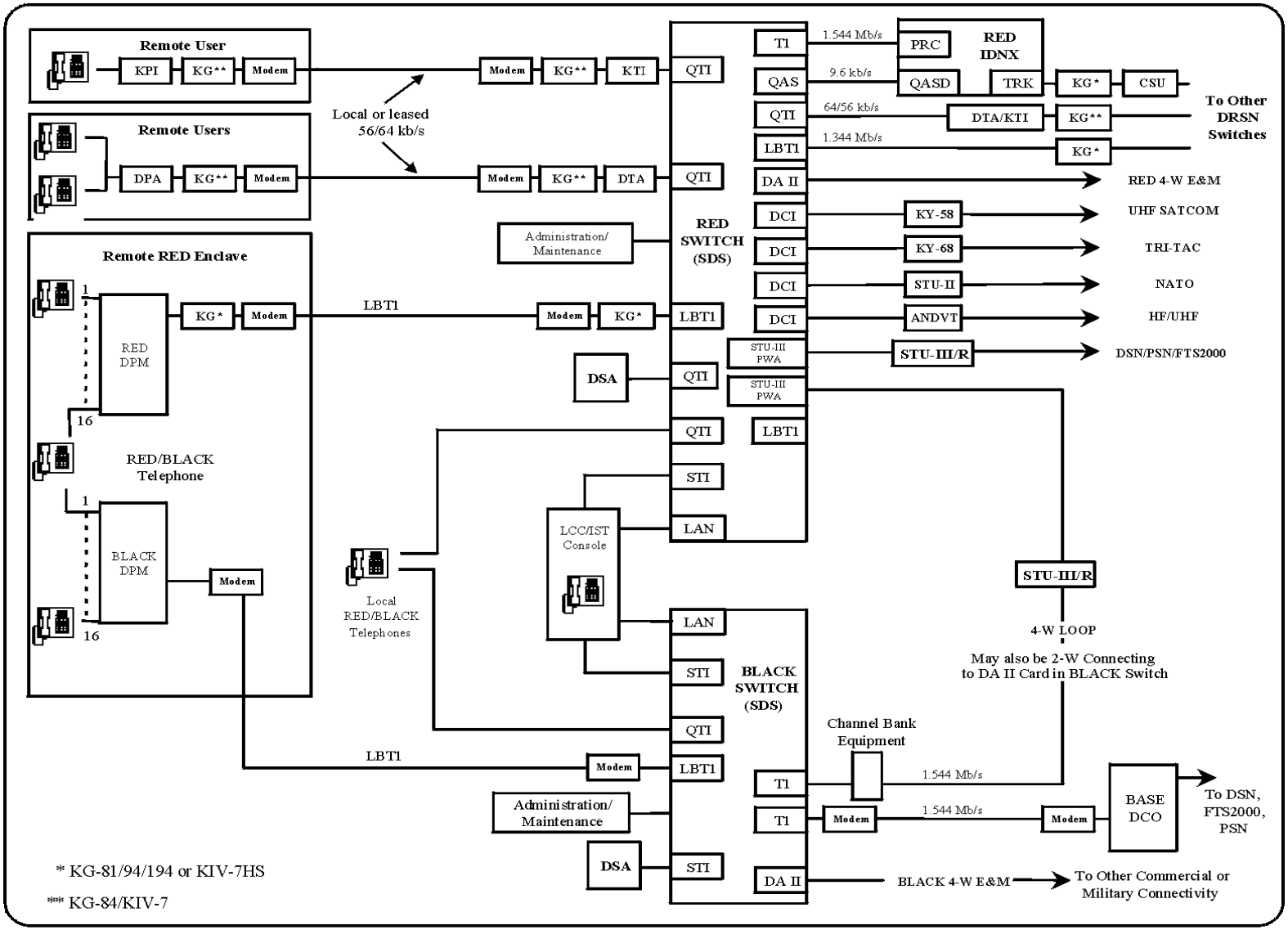

Figure 3-3. DRSN Notional System Overview

FOR OFFICIAL USE ONLY

3.1.2. Transmission Subsystem

The DRSN Transmission Subsystem provides connectivity between DRSN RED switches, connectivity between a DRSN RED switch and users located remotely from the switch, and interconnection with other secure networks and systems. The Transmission Subsystem includes Network Equipment Technologies, Inc. (N.E.T.) IDNX and Promina multiplexing equipment, encryption devices, channel service units (CSUs), and tail segment cabling. The Transmission Subsystem connects the DRSN RED switches to Government-owned and leased backbone transmission systems (e.g., full T1 or E1 transmission systems, fractional T1 (FT1) transmission links, and 56 or 64 kilobits per second (kb/s) transmission links). DRSN BLACK switch connectivity is provided by the Defense Switched Network (DSN), Public Switched Network (PSN), or Federal Telecommunications System 2000 (FTS2000), as appropriate, and is not considered a part of the DRSN Transmission Subsystem. Table 3-1 lists Integrated Digital Network Exchange (IDNX)/Promina RED and BLACK nodes that provide DRSN connectivity.

Table 3-1. DRSN Connectivity

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
Bahrain (USNAVCENT)	RS34 (RSU)	N222	D030	D045	27	D007	384 kb/s	D050	N213	N213	RS23 (RSU)	Vaihingen, GE (USEUCOM)
Bahrain (USNAVCENT)	RS34 (RSU)	N222	D030	N044	43	6XY1	1.344MB	D001	N232	N051	RS29 (SDS)	Pentagon # 1 (NMCC)
Bahrain (USNAVCENT)	RS34 (RSU)	N222	N/A	N/A	26	6I0N	384 kb/s	N/A	N/A	N220	RS20 (SDS)	MacDill AFB, FL.
Buckley (AFSPACE)	RS46 (DSS)	N223	D001	N240	10	60LB	384kb/s	D001	N059	N172	RS16 (SDS)	Cheyenne Mtn., CO (NORAD)
Buckley (AFSPACE)	RS46 (DSS)	N223	D001	N240	11	60LC	384kb/s	D001	N017	N160	RS06 (SDS)	Offutt AFB, NE #2 (USSTRATCOM HQ)
Buckley (AFSPACE)	RS46 (DSS) (DSS)	N223	D001	N240	O3	69AZ	384kb/s	D001	N066	N050	RS50 (SDS)	Schriever (AFSPACE)
Buckley (AFSPACE) (Future)	RS46 (DSS) (DSS)	N223	N/A	N/A	TBD	TBD	TBD	N/A	N/A	N/A	TBD	Onizuka, AFS
Camp Smith, HI (USPACCOM)	RS02 (RSU)	N219	N/A	N/A	10	6U0R	1.536MB	N/A	N/A	N050	RS29 (SDS)	Pentagon # 1 (NMCC)
Camp Smith, HI (USPACCOM)	RS02 (RSU)	N219	N/A	N/A	24	6Z5W	1.536MB	N/A	N/A	N240	RS01 (RSU)	Hickam AFB, HI (PACAF)
Camp Smith, HI (USPACCOM)	RS02 (RSU)	N219	D060	N131	0O	KBXE	256 kb/s	D060	N118	N235	RNOSC	Wheeler AAF, HI (RNOSC-PAC)
Camp Smith, HI (USPACCOM)	RS02 (RSU)	N219	N/A	N/A	23	6TTL	1.536MB	N/A	N/A	N240	RS54 (RSU)	Makapala, CINCPACFLT, HI
Camp Smith, HI (USPACCOM)	RS02 (RSU)	N219	D060	N131	O7	KEEX	384 kb/s	D060	N213	N232	RS37 (SDS)	Osan AB, KO (7TH AF)
Camp Smith, HI (USPACCOM)	RS02 (RSU)	N219	D060	N131	26	KEKY	384 kb/s	D060	N135	N236	RS38 (DSS)	Yongsan, KO (USFK)
Cheyenne Mtn., CO (NORAD)	RS16 (SDS)	N172	D001	N059	50	6U00	1.344MB	D001	N016	N160	RS07 (SDS)	Offutt AFB, NE #1 (USSTRATCOM CC)

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
Cheyenne Mtn., CO (NORAD)	RS16 (SDS)	N172	D001	N059	56	60LB	384 kb/s	D001	N240	N223	RS46 (DSS)	Buckley (AFSPACE)
Cheyenne Mtn., CO (NORAD)	RS16 (SDS)	N172	D001	N059	53	62AF	1.344MB	D001	N078	N180	RS25 (RSU)	Langley AFB, VA (ACC)
Cheyenne Mtn., CO (NORAD)	RS16 (SDS)	N172	D001	N059	42	6U0Z	1.344MB	D070	N183	N050	RS29 (SDS)	Pentagon #1 (NMCC)
Cheyenne Mtn., CO (NORAD)	RS16 (SDS)	N172	N/A	N/A	22	7NQ3	1.544MB	N/A	N/A	N170	RS17 (SDS)	Peterson AFB, CO (USSPACECOM)
Cheyenne Mtn., CO (NORAD)	R16 (SDS)	N172	N/A	N/A	N/A	6U54	1.344MB	N/A	N/A	N170	RS17 (SDS)	Peterson AFB, CO (USSPACECOM)
Cheyenne Mtn., CO (NORAD)	RS16 (SDS)	N172	N/A	N/A	TBD	28IP	1.344MB	N/A	N/A	N/A	DPM	Winnipeg, Canada
Cheyenne Mtn., CO (NORAD)	RS16 (SDS)	N172	D001	N059	17	611B	384 kb/s	D001	N042	N229	RS45 (DSS)	F.E. Warren AFB, WY (20TH AF)
Cheyenne Mtn., CO (NORAD)	RS16 (SDS)	N172	D001	N059	59	611D	384 kb/s	D001	N087	N228	RS44 (DSS)	Vandenberg AFB, CA (14TH AF)
Cheyenne Mtn., CO (NORAD)	RS16 (SDS)	N172	D001	N059	26	280T	256 kb/s	D060	N058	N237	RS42 (DSS)	Elmendorf AFB, AK (11TH AF)
Cheyenne Mtn., CO (NORAD)	RS16 (SDS)	N172	N/A	N/A	58	68AY	384 kb/s	N/A	N/A	N202	RS50 (SDS)	Schriever AFB AFSPACE
CMC, HQ USMC at Navy Annex	DPM	N/A	N/A	N/A	N/A	7N4T	LBT1	N/A	N/A	N051	RS29 (SDS)	Pentagon #1 (NMCC)
CP TANGO, KO	RS53 (DSS)	N239	D060	N213	22	KBW5	384 kb/s	D060	N062	N219	RS01 (RSU)	Hickam AFB, HI (PACAF)
CP TANGO, KO	RS53 (DSS)	N239	N/A	TBD	23	KBW3	512 kb/s	N/A	N/A	N236	RS38 (DSS)	Yongsan, KO (USFK)
CP TANGO, KO	RS53 (DSS)	N239	N/A	TBD	11	KBW4	384 kb/s	N/A	N/A	N232	RS37 (SDS)	Osan AB, KO (7TH AF)
Davis Monthan, AZ (12th AF)	DPM	N/A	D001	N225	N/A	7X7J	1.344MB	D001	N078	N203	RS25 (RSU)	Langley AFB, VA (ACC)
Elmendorf AFB, AK (11th AF)	RS42 (DSS)	N237	D060	N058	O6	28FX	256 kb/s	D060	N064	N219	RS01 (RSU)	Hickam AFB, HI (PACAF)

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
Elmendorf AFB, AK	RS42 (DSS)	N237	D060	N058	O7	28OT	256 kb/s	D001	N059	N172	RS16 (SDS)	Cheyenne Mtn., CO (NORAD)
EPC	(DSS)	N/A	N/A	N/A	TBD	N/A	LBT1	N/A	N050	N/A	RS29 (SDS)	Pentagon #1 (NMCC)
F.E. Warren AFB, WY (20TH AF)	RS45 (DSS)	N229	D001	N042	11	611B	384 kb/s	D001	N059	N172	RS16 (SDS)	Cheyenne Mtn., CO (NORAD)
F.E. Warren AFB, WY (20TH AF)	RS45 (DSS)	N229	D001	N042	23	611C	384 kb/s	D001	N017	N161	RS06 (SDS)	Offutt AFB, NE #2 (USSTRATCOM HQ)
Fort Buchanan, PR (USARSO)	RS49 (RSU)	N201	D080	N010	23	6G02	512 kb/s	D001	N175	N224	RS41 (RSU)	Miami, FL (USSOUTHCOM)
Fort Buchanan, PR (USARSO)	RS49 (RSU)	N201	D080	N010	22	6G03	512 kb/s	D001	N124	N200	RS26 (RSU)	Norfolk, VA (USJFCOM)
Fort Bragg, NC (18th AIRBORNE)	RS51 (DSS)	N203	D001	N139	22	69B1	512 kb/s	D001	N037	N226	RS19 (SDS)	MacDill AFB, FL #2 (USSOCOM)
Fort Bragg, NC (18th AIRBORNE)	RS51 (DSS)	N203	D001	N139	10	69B5	512 kb/s	D001	N014	N181	RS12 (RSU)	Shaw AFB, SC (9TH AF)
Fort McPherson, GA (FORSCOM)	DPM	N/A	D007	N060	11	6U0G	1.536MB	D007	N220	N/A	RS20 (SDS)	MacDill AFB, FL #1(USCENTCOM)
Fort Ritchie, MD (NMCC Site R)	RS28 (RSU)	N/A	D007	N052	27	6U0A	1.536MB	D007	N051	N/A	RS29 (SDS)	Pentagon #1 (NMCC)
Fort Ritchie, MD (NMCC Site R)	RS28 (RSU)	N/A	D007	N052	43	6U0B	1.536MB	D007	N002	N/A	RS03 (RSU)	Scott AFB, IL #2 (USTRANSCOM)
Fort Ritchie, MD (NMCC Site R)	RS28 (RSU)	N052	D001	N234	23	6U6Q	768 kb/s	D001	N017	N160	RS06 (SDS)	Offutt AFB, NE #2 (HQ USSTRATCOM)
Heidelberg, GE (USAREUR)	RS43 (DSS)	N217	D050	N213	11	D00M	512 kb/s	D050	N139	N216	RS23 (RSU)	Vaihingen, GE (USEUCOM)
Heidelberg, GE (USAREUR)	RS43 (DSS)	N217	D050	N139	23	D00N	512 kb/s	D050	N171	N210	RS22 (SDS)	Ramstein, GE (USAFE)
Heidelberg, GE (USAREUR)	RS43 (DSS)	N217	N/A	N/A	10	N/A	1.344MB	N/A	N/A	N218	RS43 (DSS)	Heidelberg, GE (USAREUR)
Hickam AFB, HI (PACAF)	RS01 (RSU)	N219	D001	N160	26	62AA	1.344MB	D060	N062	N001	RS04 (SDS)	Scott AFB, IL #1 (AMC)

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
Hickam AFB, HI (PACAF)	RS01 (RSU)	N219	D007	N/A	24	6Z5W	1.526MB	D007	N/A	N234	RS02 (RSU)	Camp Smith, HI (USPACOM)
Hickam AFB, HI (PACAF)	RS01 (RSU)	N219	D060	N118	58	KBEB	256 kb/s	D060	N062	N238	RNOSC	Wheeler AAF, HI (RNOSC-PAC)
Hickam AFB, HI (PACAF)	RS01 (RSU)	N219	D060	N062	35	KDRT	384 kb/s	D060	N213	N232	RS37 (SDS)	Osan AB, KO (7TH AF)
Hickam AFB, HI (PACAF)	RS01 (RSU)	N219	D060	N062	51	KDTN	384 kb/s	D060	N047	N230	RS05 (RSU)	Yokota AB, JA (5TH AF)
Hickam AFB, HI (PACAF)	RS01 (RSU)	N219	N/A	N/A	54	KBW5	512kb/s	N/A	N/A	N239	RS53 (DSS)	CP TANGO, KO (USFK)
Hickam AFB, HI (PACAF)	RS01 (RSU)	N219	D060	N062	42	28FX	256 kb/s	D060	N058	N237	RS42 (DSS)	Elmendorf AFB, AK (11TH AF)
HQ DISA	DPM	N205	D001	N140	N/A	6542	256kb/s	D070	N197	N051	RS29 (SDS)	Pentagon #1 (NMCC)
HQ DISA	DPM	N205	N/A	N/A	N/A	6BB8	64kb/s	N/A	N/A	N180	RS25 (RSU)	Langley AFB, VA (ACC)
Hurlburt Field, FL (AFSOC)	RS18 (RSU)	N227	D001	N050	25	6U56	1.344MB	D001	N013	N021	RS08 (RSU)	McGuire AFB, NJ (21ST AF)
Hurlburt Field, FL (AFSOC)	RS18 (RSU)	N/A	D007	N/227	24	7GET	1.536MB	D007	N226	N/A	RS19 (SDS)	MacDill AFB, FL #2 (USSOCOM)
Hurlburt Field, FL (AFSOC)	RS18 (RSU)	N227	D001	N050	42	6U6A	1.344MB	D001	N001	N001	RS04 (SDS)	Scott AFB, IL #1 (AMC)
Kelley AFB, TX (AFIC/CC)	DPA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RS29 (SDS)	Pentagon #1 (NMCC)
Kelly Barracks, GE	RS48 (DSS)	N/A	N/A	N/A	N/A	D006	N/A	N/A	N/A	N/A	RS23 (RSU)	Vaihingen, GE (USEUCOM)
Kunsan AB, KO (8TH TFW)	RS35 (DSS)	N/A	D007	N233	O3	KCTA	384 kb/s	D007	N232	N/A	RS37 (SDS)	Osan AB, KO (7TH AF)
Kunsan AB, KO (8TH TFW)	RS35 (DSS)	N/A	D007	N233	O6	KEMN	384 kb/s	D007	N236	N/A	RS38 (DSS)	Yongsan AB, KO (USFK)
Langley AFB, VA (ACC)	RS25 (RSU)	N180	D001	N053	27	62AE	1.344MB	D001	N014	N180	RS12 (RSU)	Shaw AFB, SC (9TH AF)

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
Langley AFB, VA (ACC)	RS25 (RSU)	N180	D001	N078	10	62AF	1.344MB	D001	N059	N172	RS16 (SDS)	Cheyenne Mtn., CO (NORAD)
Langley AFB, VA (ACC)	RS25 (RSU)	N180	D001	N078	24	62AG	1.344MB	D001	N183	N051	RS29 (SDS)	Pentagon #1 (NMCC)
Langley AFB, VA (ACC)	RS25 (RSU)	N/A	D001	N078	N/A	7X7J	1.344MB	D001	N225	N/A	DPM	Davis Monthan, AZ (12TH AF)
London, UK (USNAVEUR)	RS39 (RSU)	N214	D050	N189	22	W9HU	512 kb/s	D050	N213	N216	RS23 (RSU)	Vaihingen, GE (USEUCOM)
London, UK (USNAVEUR)	RS39 (RSU)	N214	D050	N189	10	WNF1	512 kb/s	D050	N174	N212	RS47 (DSS)	SHAPE, Belgium (SHAPE)
London, UK (USNAVEUR)	RS39 (RSU)	N214	D050	N189	11	D00G	256 kb/s	D050	N171	N210	RS22 (SDS)	Ramstein AB, GE (USAFE)
MacDill AFB, FL #1 (USCENTCOM)	RS20 (SDS)	N220	D001	N247	57	6U31	1.344MB	D050	N214	N216	RS23 (RSU) (RSU)	Vaihingen, GE (USEUCOM)
MacDill AFB, FL #1 (USCENTCOM)	RS20 (SDS)	N220	D001	N247	55	62AK	1.344MB	D001	N014	N181	RS12 (RSU)	Shaw AFB, SC (9TH AF)
MacDill AFB, FL #1 (USCENTCOM)	RS20 (SDS)	N220	D001	N247	23	6U1C	1.344MB	D070	N197	N050	RS27 (RSU)	Pentagon #2 (OSD/ESC)
MacDill AFB, FL #1 (USCENTCOM)	RS20 (SDS)	N/A	D007	N220	41	6U07	1.536MB	D007	N226	N/A	RS19 (SDS)	MacDill AFB, FL #2 (USSOCOM)
MacDill AFB, FL #1 (USCENTCOM)	RS20 (SDS)	N/A	D007	N220	40	6U0K	1.536MB	D007	N200	N/A	RS26 (RSU)	Norfolk, VA (USJFCOM)
MacDill AFB, FL #1 (USCENTCOM)	RS20 (SDS)	N/A	D007	N220	24	6U0G	1.536MB	D007	N060	N/A	DPM	Fort McPherson, GA (FORSCOM)
MacDill AFB, FL #2 (USSOCOM)	RS19 (SDS)	N/A	D007	N226	26	6U07	1.536MB	D007	N220	N/A	RS20 (SDS)	MacDill AFB, FL #1 (USCENTCOM)
MacDill AFB, FL #2 (USSOCOM)	RS19 (SDS)	N/A	D007	N226	25	7GET	1.536MB	D007	N227	N/A	RS18 (RSU)	Hurlburt Field, FL (AFSOC)
MacDill AFB, FL #2 (USSOCOM)	RS19 (SDS)	N226	D001	N037	20	69B1	512 kb/s	D001	N139	N203	RS51 (DSS)	Fort Bragg, NC (18th AIRBORNE)

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
MacDill AFB, FL #2 (USSOCOM)	RS19 (SDS)	N226	D001	N037	39	6U02	1.344MB	D001	N001	N001	RS04 (SDS)	Scott AFB, IL #1 (AMC)
MacDill AFB, FL #2 (USSOCOM)	RS19 (SDS)	N226	D001	N037	36	28X8	512 kb/s	D001	N175	N224	RS41 (RSU)	Miami, FL (USSOUTHCOM)
Makalapa (SBIRS)	RS54 (RSU)	N/A	D007	N240	43	6TTK	1.536MB	D007	N219	N/A	RS01 (RSU)	Hickam AFB, HI (PACAF)
Makalapa (SBIRS)	RS54 (RSU)	N/A	D007	N240	23	6TTL	1.536MB	D007	N234	N/A	RS02 (RSU)	Camp Smith, HI (USPACOM)
Maxwell AFB, AL (AU/CC)	DPA	N/A	D001	N057	N/A	7Z8C	56 kb/s	D001	N043	N/A	RS29 (SDS)	Pentagon #1 (NMCC)
McGuire AFB, NJ (21ST AF)	RS08 (RSU)	N021	D001	N013	25	6U56	1.344MB	D001	N050	N227	RS18 (RSU)	Hurlburt Field, FL (AFSOC)
McGuire AFB, NJ (21ST AF)	RS08 (RSU)	N021	D001	N013	O9	6U53	1.344MB	D001	N052	N022	RS14 (RSU)	Travis AFB, CA (15TH AF)
McGuire AFB, NJ (21ST AF)	RS08 (RSU)	N021	D001	N013	11	6U55	1.344MB	D001	N001	N001	RS04 (SDS)	Scott AFB, IL #1 (AMC)
Miami, FL (USSOUTHCOM)	RS41 (RSU)	N224	D001	N175	40	28X9	512 kb/s	D001	N124	N200	RS26 (RSU)	Norfolk, VA (USJFCOM)
Miami, FL (USSOUTHCOM)	RS41 (RSU)	N224	D001	N175	25	28X8	512 kb/s	D001	N037	N226	RS19 (SDS)	MacDill AFB, FL #2 (USSOCOM)
Miami, FL (USSOUTHCOM)	RS41 (RSU)	N224	D001	N175	41	6G02	512 kb/s	D080	N010	N201	RS49 (RSU)	Fort Buchanan, PR (USARSO)
Misawa AB, JA (432ND TFW)	RS24 (RSU)	N231	D060	N048	O8	KBPE	384 kb/s	D060	N177	N230	RS05 (RSU)	Yokota AB, JA (5TH AF)
Misawa AB, JA (432ND TFW)	RS24 (RSU)	N/A	D007	N200	DPA	28R2	56 kb/s	D007	N/A	N/A	RS05 (RSU)	Yokota AB, JA (5TH AF)
Naples, IT (USNAVEUR)	RS31 (RSU)	N215	D050	N216	42	D00E	512 kb/s	D050	N213	N216	RS23 (RSU)	Vaihingen, GE (USEUCOM)
Naples, IT (USNAVEUR)	RS31 (RSU)	N215	D050	N216	25	D00F	512 kb/s	D050	N171	N210	RS22 (SDS)	Ramstein AB, GE (USAFE)
Navy Command Center (Pentagon)	DPM	N/A	N/A	N/A	N/A	28LD	N/A	N/A	N/A	N/A	RS29 (SDS)	Pentagon #1 (NMCC)

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
Norfolk, VA (USJFCOM)	RS26 (RSU)	N/A	D007	N200	14	6U0K	1.536MB	D007	N220	N/A	RS20 (SDS)	MacDill AFB, FL #1 (USCENTCOM)
Norfolk, VA (USJFCOM)	RS26 (RSU)	N/A	D007	N200	O9	6U0J	1.536MB	D007	N051	N/A	RS29 (SDS)	Pentagon #1 (NMCC)
Norfolk, VA (USJFCOM)	RSS6 (RSU)	N200	D001	N124	12	6G03	512 kb/s	D080	N010	N201	RS49 (RSU)	Fort Buchanan, PR (USARSO)
Norfolk, VA (USJFCOM)	RS26 (RSU)	N200	D001	N124	13	28X9	512 kb/s	D001	N175	N224	RS41 (RSU)	Miami, FL (USSOUTHCOM)
Offutt AFB, NE #1 (USSTRATCOM CC)	RS07 (SDS)	N/A	N/A	N160	24	N/A	1.544MB	N/A	N161	N/A	RS06 (SDS)	Offutt AFB, NE #2 (USSTRATCOM HQ)
Offutt AFB, NE #1 (USSTRATCOM CC)	RS07 (SDS)	N/A	N/A	N160	O8	N/A	1.544MB	N/A	N161	N/A	RS06 (SDS)	Offutt AFB, NE #2 (USSTRATCOM HQ)
Offutt AFB, NE #1 (USSTRATCOM CC)	RS07 (SDS)	N160	D001	N017	16	6U1B	1.344MB	D070	N097	N051	RS29 (SDS)	Pentagon #1 (NMCC)
Offutt AFB, NE #1 (USSTRATCOM CC)	RS07 (SDS)	N/A	N/A	N160	O4	6U6Q	768kb/s	N/A	N052	N/A	RS28 (RSU)	Site R (NMCC)
Offutt AFB, NE #1 (USSTRATCOM CC)	RS07 (SDS)	N160	D001	N016	26	6U00	1.344MB	D001	N059	N172	RS16 (SDS)	Cheyenne Mtn., CO (NORAD)
Offutt AFB, NE #1 (USSTRATCOM CC)	RS07 (SDS)	N/A	N/A	N/A	N/A	N/A	2EA	N/A	N/A	N/A	DSS	WWSVCS-DSS-1 Offutt AFB, NE
Offutt AFB, NE #2 (USSTRATCOM HQ)	RS06 (SDS)	N/A	N/A	N161	O5	N/A	1.544MB	N/A	N160	N/A	RS07 (SDS)	Offutt AFB, NE #1 (USSTRATCOM CC)
Offutt AFB, NE #2 (USSTRATCOM HQ)	RS06 (SDS)	N/A	N/A	N161	21	N/A	1.544MB	N/A	N160	N/A	RS07 (SDS)	Offutt AFB, NE #1 (USSTRATCOM CC)
Offutt AFB, NE #2 (USSTRATCOM HQ)	RS06 (SDS)	N161	D001	N017	O8	60LC	384 kb/s	D001	N240	N223	RS46 (DSS)	Buckley (AFSPACE)

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
Offutt AFB, NE #2 (USSTRATCOM HQ)	RS06 (SDS)	N161	D001	N017	26	6U01	1.344MB	D001	N001	N001	RS04 (SDS)	Scott AFB, IL #1 (AMC)
Offutt AFB, NE #2 (USSTRATCOM HQ)	RS06 (SDS)	N/A	N/A	N/A	N/A	N/A	2EA	N/A	N/A	N/A	DSS	WWSVCS-DSS-1 Offutt AFB, NE
Offutt AFB, NE #2 (USSTRATCOM HQ)	RS06 (SDS)	N161	D001	N017	18	611C	384 kb/s	D001	N042	N229	RS45 (DSS)	F.E. Warren AFB, WY (20TH AF)
Offutt AFB, NE #2 (USSTRATCOM HQ)	RS06 (SDS)	N161	D001	N017	O6	611E	384 kb/s	D001	N087	N228	RS44 (DSS)	Vandenberg AFB, CA (14TH AF)
Osan AB, KO (7TH AF)	RS37 (SDS)	N232	D060	N213	38	KDRT	384 kb/s	D060	N062	N219	RS01 (RSU)	Hickam AFB, HI (PACAF)
Osan AB, KO (7TH AF)	RS37 (SDS)	N232	D060	N213	34	KCHC	384 kb/s	D060	N194	N236	RS38 (DSS)	Yongsan AB (USFK)
Osan AB, KO (7TH AF)	RS37 (SDS)	N232	D060	N213	18	KEEX	384 kb/s	D060	N131	N234	RS02 (RSU)	Camp Smith, HI (USPACOM)
Osan AB, KO (7TH AF)	RS37 (SDS)	N/A	D007	N232	19	KCTA	384 kb/s	D007	N233	N/A	RS35 (DSS)	Kunsan AFB, KO (8TH TFW)
Osan AB, KO (7TH AF)	RS37 (SDS)	N/A	N/A	N232	21	KBW4	512kb/s	N/A	N239	N/A	RS53 (DSS)	CP TANGO, KO
Osan AB, KO (7TH AF)	RS37 (SDS)	N232	D060	N213	22	KBPD	384 kb/s	D060	N047	N230	RS05 (RSU)	Yokota AB, JA (5TH AF)
Pentagon #1 (NMCC)	RS29 (SDS)	N051	D070	N183	27	62AG	1.344MB	D001	N078	N180	RS25 (RSU)	Langley AFB, VA (ACC)
Pentagon #1 (NMCC)	RS29 (SDS)	N051	D070	N197	59	62AC	1.344MB	D050	N171	N210	RS22 (SDS)	Ramstein AB, GE (USAFE)
Pentagon #1 (NMCC)	RS29 (SDS)	N051	D070	N183	24	62AJ	1.344MB	D001	N021	N225	RS09 (RSU)	Wright-Patterson AFB, OH (AFMC)
Pentagon #1 (NMCC)	RS29 (SDS)	N051	D070	N197	73	6U1B	1.344MB	D001	N017	N160	RS07 (SDS)	Offutt AFB, NE #1 (USSTRATCOM CC)
Pentagon #1 (NMCC)	RS29 (SDS)	N051	D070	N183	57	6U1A	1.344MB	D001	N051	N002	RS03 (RSU)	Scott AFB, IL #2 (USTRANSCOM)

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
Pentagon #1 (NMCC)	RS27 (RSU)	N051	D070	N197	26	62AH	1.344MB	D001	N001	N001	RS04 (SDS)	Scott AFB, IL #1 (AMC)
Pentagon #1 (NMCC)	RS29 (SDS)	N/A	D007	N051	41	6U0A	1.536MB	D007	N052	N/A	RS28 (RSU)	Fort Ritchie, MD (NMCC Site R)
Pentagon #1 (NMCC)	RS29 (SDS)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RS27 (RSU)	Pentagon #2 (OSD/ESC)
Pentagon #1 (NMCC)	RS29 (SDS)	N/A	N/A	N/A	N/A	RD72	1.544MB	N/A	N/A	N/A	DSS	State Dept.
Pentagon #1 (NMCC)	RS29 (SDS)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	DSS	EPC
Pentagon #1 (NMCC)	RS29 (SDS)	N/A	N/A	N/A	N/A	7N4T	1.544MB	N/A	N/A	N/A	DPM	CMC, HQ USMC At Navy Annex
Pentagon #1 (NMCC)	RS29 (SDS)	N/A	N/A	N/A	N/A	28LD	1.544MB	N/A	N/A	N/A	DPM	Navy CC
Pentagon #1 (NMCC)	RS29 (SDS)	N/A	D070	N197	N/A	6U59	1.344MB	D001	N140	N/A	DPM	HQ DISA
Pentagon #1 (NMCC)	RS29 (SDS)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	DSS	Pentagon Secure Conf System (PSCS)
Pentagon #1 (NMCC)	RS29 (SDS)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	DSS	WWSVCS
Pentagon #1 (NMCC)	RS29 (SDS)	N/A	D070	N197	N/A	7Z8B	56 kb/s	D001	N006	N/A	DPA	Randolph AFB, TX (AETC/CC)
Pentagon #1 (NMCC)	RS29 (SDS)	N/A	D007	N051	72	6U0J	1.536MB	D007	N200	N/A	RS26 (RSU)	Norfolk, VA (USJFCOM)
Pentagon #2 (OSD/ESC)	RS29 (SDS)	N/A	D007	N050	O7	6U0R	1.536MB	D007	N234	N/A	RS02 (RSU)	Camp Smith, HI (USPACOM)
Pentagon #2 (OSD/ESC)	RS29 (SDS)	N050	D070	N183	O6	6U0Z	1.344MB	D001	N059	N172	RS16 (SDS)	Cheyenne Mtn., CO (NORAD)
Pentagon #2 (OSD/ESC)	RS27 (RSU)	N050	D070	N197	O8	6U1C	1.344MB	D001	N247	N220	RS20 (SDS)	MacDill AFB, FL #1 (USCENTCOM)
Pentagon #2 (OSD/ESC)	RS27 (RSU)	N/A	N/A	N050	O9	6U32	1.344MB	N/A	N216	N/A	RS23 (RSU)	Vaihingen, GE (USEUCOM)

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
Pentagon #2 (OSD/ESC)	RS27 (RSU)	N/A	N/A	N/A	N/A	20DV	N/A	N/A	N/A	N/A	N/A	WHCA
Pentagon #2 (OSD/ESC)	RS27 (RSU)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RS29 (SDS)	Pentagon #1 (NMCC)
Pentagon #2 (OSD/ESC)	RS27 (RSU)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N	N/A	RS29 (SDS)	Pentagon #1 (NMCC)
(PSCS)	DSS	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RS29 (SDS)	Pentagon #1 (NMCC)
Peterson AFB, CO (USSPACECOM)	RS17 (SDS)	N170	D001	N028	22	6U09	1.344MB	D001	N001	N001	RS04 (SDS)	Scott AFB, IL #1 (AMC)
Peterson AFB, CO (USSPACECOM)	RS17 (SDS)	N/A	D007	N170	58	7NQ3	1.536MB	D007	N172	N/A	RS16 (SDS)	Cheyenne Mtn., CO (NORAD)
Peterson AFB, CO (USSPACECOM)	RS17 (SDS)	N/A	D007	N170	N/A	6U54	1.544MB	D007	N172	N/A	RS16 (SDS)	Cheyenne Mtn., CO (NORAD)
Ramstein AB, GE (USAFE)	RS22 (SDS)	N210	D050	N171	16	62AB	1.344MB	D001	N001	N001	RS04 (SDS)	Scott AFB, IL #1 (AMC)
Ramstein AB, GE (USAFE)	RS22 (SDS)	N210	D050	N171	56	62AC	1.344MB	D070	N197	N051	RS29 (SDS)	Pentagon #1 (NMCC)
Ramstein AB, GE (USAFE)	RS22 (SDS)	N210	D050	N171	41	W9FV	1.344MB	D050	N214	N216	RS23 (RSU)	Vaihingen, GE (USEUCOM)
Ramstein AB, GE (USAFE)	RS22 (SDS)	N210	D050	N171	40	D00G	512 kb/s	D050	N189	N214	RS39 (RSU)	London, UK (USNAVEUR)
Ramstein AB, GE (USAFE)	RS22 (SDS)	N210	D050	N171	25	D00F	512 kb/s	D050	N016	N215	RS31 (RSU)	Naples, IT (USNAVEUR)
Ramstein AB, GE (USAFE)	RS22 (SDS)	N210	D050	N171	38	D00N	512 kb/s	D050	N139	N217	RS43 (DSS)	Heidelberg, GE (USAREUR)
Ramstein AB, GE (USAFE)	RS22 (SDS)	N210	D050	N142	43	D004	384 kb/s	D050	N174	N212	RS47 (DSS)	SHAPE, BE (SHAPE)
Randolph AFB, TX (AETC/CC)	DPA	N/A	D001	N006	N/A	7Z8B	56 kb/s	D070	N197	N/A	RS29 (SDS)	Pentagon #1 (NMCC)
Scott AFB, IL #1 (AMC)	RS04 (SDS)	N001	D001	N001	42	O361	1.344MB	D001	N005	N249	RNOSC	Scott AFB, IL

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
Scott AFB, IL #1 (AMC)	RS04 (SDS)	N/A	N/A	N001	26	O301	1.544MB	N/A	N002	N/A	RS03 (RSU)	Scott AFB, IL
Scott AFB, IL #1 (AMC)	RS04 (SDS)	N001	D001	N001	70	62AB	1.344MB	D050	N171	N210	RS22 (SDS)	Ramstein AB, GE (USAFE)
Scott AFB, IL #1 (AMC)	RS04 (SDS)	N001	D001	N001	24	6U55	1.344MB	D001	N013	N021	RS08 (RSU)	McGuire AFB, NJ (21ST AF)
Scott AFB, IL #1 (AMC)	RS04 (SDS)	N001	D001	N001	41	6U01	1.344MB	D001	N017	N161	RS06 (SDS)	Offutt AFB, NE #2 (USSTRATCOM HQ)
Scott AFB, IL #1 (AMC)	RS04 (SDS)	N001	D001	N001	58	6U57	1.344MB	D001	N052	N022	RS14 (RSU)	Travis AFB, CA (15TH AF)
Scott AFB, IL #1 (AMC)	RS04 (SDS)	N001	D001	N001	53	6U09	1.344MB	D001	N028	N170	RS17 (SDS)	Peterson AFB, CO (USSPACECOM)
Scott AFB, IL #1 (AMC)	RS04 (SDS)	N001	D001	N001	22	62AA	1.344MB	D060	N062	N219	RS01 (RSU)	Hickam AFB, HI (PACAF)
Scott AFB, IL #1 (AMC)	RS04 (SDS)	N001	D001	N001	25	6U02	1.344MB	D001	N037	N226	RS19 (SDS)	MacDill AFB, FL #2 (USSOCOM)
Scott AFB, IL #1 (AMC)	RS04 (SDS)	N001	D001	N001	40	6U6A	1.344MB	D001	N050	N227	RS18 (RSU)	Hurlburt Field, FL (AFSOC)
Scott AFB, IL #1 (AMC)	RS04 (SDS)	N001	D001	N001	55	62AH	1.344MB	D070	N197	N051	RS27 (RSU)	Pentagon #1 (NMCC)
Scott AFB, IL #2 (USTRANSCOM)	RS03 (RSU)	N002	D001	N051	O8	6U1A	1.344MB	D070	N183	N051	RS29 (SDS)	Pentagon #1 (NMCC)
Scott AFB, IL #2 (USTRANSCOM)	RS03 (RSU)	N/A	D007	N002	O9	6U0B	1.536MB	D007	N052	N/A	RS28 (RSU)	Fort Ritchie, MD (NMCC Site R)
Scott AFB, IL #2 (USTRANSCOM)	RS03 (RSU)	N/A	N/A	N/A	24	O301	1.544MB	N/A	N002	N/A	RS04 (SDS)	Scott AFB, IL #1 (AMC)
Scott AFB, IL #2 (USTRANSCOM)	RS03 (RSU)	N/A	D007	N002	25	6U2H	1.344MB	D050	N250	N/A	RNOSC	Scott AFB, IL
SHAPE, BE (SHAPE)	RS47 (DSS)	N212	D050	N174	7	D004	384 kb/s	D050	N142	N210	RS22 (SDS)	Ramstein AB, GE (USAFE)
SHAPE, BE (SHAPE)	RS47 (DSS)	N212	D050	N174	10	WNF1	512 kb/s	D050	N189	N214	RS39 (RSU)	London, UK (USNAVEUR)

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
SHAPE, BE (SHAPE)	RS47 (DSS)	N212	D050	N174	11	WNF7	384 kb/s	D050	N214	N216	RS23 (RSU)	Vaihingen, GE (USEUCOM)
Shaw AFB, SC (9TH AF)	RS12 (RSU)	N181	D001	N014	24	62AK	1.344MB	D001	N247	N220	RS20 (SDS)	MacDill AFB, FL #1 (USCENTCOM)
Shaw AFB, SC (9TH AF)	RS12 (RSU)	N181	D001	N014	41	62AE	1.344MB	D001	N053	N180	RS25 (RSU)	Langley AFB, VA (ACC)
Shaw AFB, SC (9TH AF)	RS12 (RSU)	N181	D001	N014	23	69B5	512 kb/s	D001	N139	N203	RS51 (DSS)	Fort Bragg, NC (18th AIRBORNE)
State Dept.	N/A	N/A	N/A	N/A	N/A	RD72	1.544MB	N/A	N/A	N/A	RS29 (SDS)	Pentagon #1 (NMCC)
Travis AFB, CA (15TH AF)	RS14 (RSU)	N022	D001	N052	40	6U53	1.344MB	D001	N013	N021	RS08 (RSU)	McGuire AFB, NJ (21ST AF)
Travis AFB, CA (15TH AF)	RS14 (RSU)	N022	D001	N052	25	6U57	1.344MB	D001	N001	N001	RS04 (SDS)	Scott AFB, IL #1 (AMC)
Vaihingen, GE (USEUCOM)	RS23 (RSU)	N216	D050	N214	24	6U31	1.344MB	D001	N247	N220	RS20 (SDS)	MacDill AFB, FL #1 (USCENTCOM)
Vaihingen, GE (USEUCOM)	RS23 (RSU)	N216	D050	N214	25	W9FV	1.344MB	D050	N171	N210	RS22 (SDS)	Ramstein AB, GE (USAFE)
Vaihingen, GE (USEUCOM)	RS23 (RSU)	N216	D050	N213	40	6U32	1.344MB	D070	N183	N051	RS29 (SDS)	Pentagon #1 (NMCC)
Vaihingen, GE (USEUCOM)	RS23 (RSU)	N216	D050	N213	26	W9HU	512 kb/s	D050	N189	N214	RS39 (RSU)	London, UK (USNAVEUR)
Vaihingen, GE (USEUCOM)	RS23 (RSU)	N216	D050	N213	41	D00E	512 kb/s	D050	N216	N215	RS31 (RSU)	Naples, IT (USNAVEUR)
Vaihingen, GE (USEUCOM)	RS23 (RSU)	N216	D050	N213	58	DOOM	512 kb/s	D050	N139	N217	RS43 (DSS)	Heidelberg, GE (USAREUR)
Vaihingen, GE (USEUCOM)	RS23 (RSU)	N216	D050	N213	57	D007	384 kb/s	D050	N045	N222	RS34 (RSU)	Bahrain (USNAVCENT)
Vaihingen, GE (USEUCOM)	RS23 (RSU)	N216	D050	N214	42	WNF7	384 kb/s	D050	N174	N212	RS47 (DSS)	SHAPE, BE (SHAPE)
Vaihingen, GE (USEUCOM)	RS23 (RSU)	N/A	N/A	N/A	N/A	D006	N/A	N/A	N/A	N/A	RS48 (DSS)	Kelly Barracks, GE

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
Vandenberg AFB, CA (14TH AF)	RS44 (DSS)	N228	D001	N087	11	611D	384 kb/s	D001	N059	N172	RS16 (SDS)	Cheyenne Mtn., CO (NORAD)
Vandenberg AFB, CA (14TH AF)	RS44 (DSS)	N228	D001	N087	10	611E	384 kb/s	D001	N017	N161	RS06 (SDS)	Offutt AFB, NE #2 (USSTRATCOM HQ)
WHCA	N/A	N/A	N/A	N/A	N/A	20DV	N/A	N/A	N/A	N/A	RS27 (RSU)	Pentagon #2 (OSD/ESC)
Wheeler AAF, HI (RNOSC-PAC)	RNOSC	N235	D060	N118	OO	KBXE	256 kb/s	D060	N131	N234	RS02 (RSU)	Camp Smith, HI (USPACOM)
Wheeler AAF, HI (RNOSC-PAC)	RNOSC	N235	D060	N118	16	KBEB	256 kb/s	D060	N062	N235	RS01 (RSU)	Hickam AFB, HI (PACAF)
Winnipeg, Canada	DPM (DSS)	N/A	D007	N/A	N/A	281P	1.344MB	D007	N172	N/A	RS16 (SDS)	Cheyenne Mtn., CO (NORAD)
Wright-Patterson AFB, OH (AFMC)	RS09 (RSU)	N225	D001	N021	O9	62AJ	1.344MB	D070	N183	N051	RS29 (SDS)	Pentagon #1 (NMCC)
Wright-Patterson AFB, OH (AFMC)	RS09 (RSU)	N/A	D001	N225	N/A	7R20	56 kb/s	D001	N001	N/A	RS04 (SDS)	Scott AFB, IL #1 (AMC)
WWSVCS	DSS	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RS07 (SDS)	Offutt AFB, NE #1 (USSTRATCOMCC)
WWSVCS	DSS	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RS06 (SDS)	Offutt AFB, NE #2 (USSTRATCOM HQ)
WWSVCS	DSS	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RS29 (SDS)	Pentagon #1 (NMCC)
Yokota AB, JA (5TH AF)	RS05 (RSU)	N230	D060	N048	O8	KBPE	384 kb/s	D060	N177	N231	RS24 (RSU)	Misawa AB, JA (432ND TFW)
Yokota AB, JA (5TH AF)	RS05 (RSU)	N230	D060	N047	O7	KBPD	384 kb/s	D060	N213	N232	RS37 (SDS)	Osan AB, KO (USFK)
Yokota AB, JA (5TH AF)	RS05 (RSU)	N230	D060	N047	24	KDTN	384 kb/s	D060	N062	N219	RS01 (RSU)	Hickam AFB, HI (PACAF)
Yokota AB, JA (5TH AF)	RS05 (RSU)	N/A	D007	N/A	N/A	28R2	56 kb/s	D007	N/A	N/A	RS24 (RSU)	Misawa, JA (432ND TFW)
Yongsan, KO (USFK)	RS38 (DSS)	N236	N194	D060	15	KCHC	384 kb/s	D060	N213	N232	RS37 (SDS)	Osan AB, KO (7TH AF)

FOR OFFICIAL USE ONLY

LOCATION	SWITCH TYPE	RED IDNX NODE	BLACK DOMAIN	BLACK IDNX NODE	TRUNK CARD	CCSD	TYPE	BLACK DOMAIN	BLACK IDNX NODE	RED IDNX NODE	SWITCH TYPE	LOCATION
Yongsan, KO (USFK)	RS38 (DSS)	N/A	N236	D007	O6	KEMN	384 kb/s	D007	N233	N/A	RS35 (DSS)	Kunsan AFB, KO (8TH TFW)
Yongsan, KO (USFK)	RS38 (DSS)	N/A	N236	N/A	18	KBW3	512 kb/s	N/A	N239	N/A	RS53 (DSS)	CP TANGO, KO
Yongsan, KO (USFK)	RS38 (DSS)	N236	D060	N135	O3	KEKY	384 kb/s	D060	N131	N234	RS02 (RSU)	Camp Smith, HI (USPACOM)

FOR OFFICIAL USE ONLY

3.1.3. Timing and Synchronization Subsystem

The T&S Subsystem is comprised of reference clocks, clock distribution systems, and RED/BLACK isolation filters and buffers. The T&S Subsystem provides a primary, secondary, and tertiary method of obtaining a timing source for site contingency and the network.

3.1.4. Network Management Subsystem

The NMS provides DISA with the capabilities to provide day-to-day direction and operational oversight of the DRSN. It includes the facilities, equipment, organizational structure, and people to monitor and interface with the DRSN site O&M activity to affect problem resolution.

Intentionally left blank

SECTION 4
DRSN NETWORK MANAGEMENT

4.1 GENERAL

DISA, as the Joint Staff designated System Manager (SM) for the DRSN, is responsible for providing operational direction and management of worldwide DRSN assets.

4.1.1 Network Management Subsystem

Network management requirements for the DRSN are specified in the Joint Staff Memorandum J-6A 016650-92, *Secure Voice Requirements Concept,* which is under going revision. NM ensures user-to-user service is maintained under changing traffic conditions, changing user requirements, natural and manufactured stresses and disturbances, and equipment failures or degradations. NM consists of the following five functions:

- Fault Management (FM)
- Performance Management (PM)
- Configuration Management (CM)
- Security Management (SM)
- Accounting Management (AM)

O&M personnel play a major part in enhancing the day-to-day and long-term network performance through the collection of network performance and configuration data and assisting in the detection, diagnosis, and correction of performance problems at the site level.

4.1.2 Fault Management

Fault management is defined as the detection, isolation, and correction of network problems. It encompasses activities such as performing system diagnostics, tracing faults through a network, managing error logs, identifying causative events, and correcting faults.

Fault management provides centralized near-real-time management of the network during times of abnormal traffic conditions and/or equipment failures to ensure the network can be optimized to support critical command and control traffic under stress conditions.

The Regional Network Operations and Security Centers (RNOSCs) and O&M sites support FM by continuously monitoring DRSN alarm ports, processing received data, maintaining event logs, and notifying the site operator when significant alarms occur in DRSN subsystems.

4.1.3 Performance Management

Performance management is defined as the collection and analysis of statistical data to measure the performance of a network. Performance management permits the use of models to determine whether a network element is:

- Meeting required throughput rates
- Providing adequate response times
- Approaching overload conditions
- Operating efficiently

The RNOSCs and O&M sites support PM by gathering performance data and developing statistics to diagnose day-to-day network problems or abnormalities. The PM data is also used to support long-term network sizing and topology design studies.

4.1.4 Configuration Management

Network CM ensures changes to the DRSN baseline are methodically approved and controlled. Configuration management begins with the implementation of the approved network functional baseline. Configuration management reviews approves or disapproves change proposals, deviations, and waivers to the baseline. Configuration management also oversees implementation of the baseline and approved changes and audits the network functionality to ensure compliance with the baseline and approved changes.

The RNOSCs and O&M sites support CM through the establishment and maintenance of a network CM database. Centralized management and configuration control of network features, such as network routing, numbering, precedence levels, security access levels (SALs), calling area authorizations, and alarm classifications, ensure standardization that simplifies user operational procedures and enhances network performance.

4.1.5 Accounting Management

Accounting management (AM) defines how network usage, charges, and costs are identified. Accounting management allows users and managers to place limits on usage and to negotiate additional resources where needed.

The RNOSCs and O&M sites support AM by providing network user data for billing purposes through the CM database.

4.1.6 Security Management

Security management is concerned with protecting managed objects. It provides cryptographic key management, authentication rules, access control routines, authorization facility maintenance, and security logs.

4.2 NETWORK MANAGEMENT RESPONSIBILITIES

The following is a description of the DRSN NM hierarchy and overall responsibilities.

4.2.1 DISA Program Management Office

The DRSN Program Management Office is responsible for non-real-time operational management of the DRSN, including development of operational policy and procedures, operational CM, long-term performance analysis, and circuit provisioning. The Program Management Office also operates a DRSN EBBS to provide on-line access to DRSN information, such as the *DRSN Telephone Directory*, points of contact (POCs), Engineering Change Proposal (ECP) status, and other information related to DRSN O&M.

The Program Management Office also receives a feed from the Scott AFB, IL, RNOSC Advanced RED Defense Integrated Management Support System (ARDIMSS) database. This information covers all DRSN switch fault alarms for a 24-hour period. It is used to look for trends coming from the DRSN and specific outages on VIP telephones. The Program Management Office works closely with the RNOSCs and, occasionally, with switch site personnel to identify problems and trends and correct deficiencies attempting to prevent major outages or disruptions to VIP customers.

4.2.2 National Military Command Center Communications Watch Division

The NMCC Communications Watch Division (CWD) maintains a worldwide view of the DRSN and reports to the NCA any conditions that could impair the ability to support worldwide contingency operations. The CWD notifies the GNOSC and the Scott RNOSC of failures, NMCC VIP call failures, outages, degradations, or any problems identified by the NMCC with the potential for affecting service to a senior DRSN customer of Joint Staff interest.

4.2.3 DISA Global Network Operations and Security Center

The Global Network Operations and Security Center (GNOSC) maintains a worldwide view of the entire DRSN as well as all other DISA managed (i.e., DISN) networks. The GNOSC assesses and coordinates resolution of intertheater network problems and advises key personnel of network status.

4.2.4 DISA Regional Network Operations and Security Centers and DRSN Operations Center

The Scott AFB, RNOSC and the RNOSCs in Vaihingen (Patch Barracks), Germany, Europe (EUR) and the Wheeler Army Air Field (AAF), HI, Pacific (PAC) provide day-to-day oversight and management of DRSN assets in their areas of responsibility. The Scott, EUR and PAC RNOSCs maintain continuous surveillance of DRSN assets in their assigned region to detect abnormalities, to implement or direct near-real-time corrective actions in response to adverse network conditions, and to coordinate repair and restoration actions with the military department

(MILDEP) O&M Commands. They also coordinate authorized outages with the O&Ms and report network conditions to the GNOSC. In addition, the Scott RNOSC coordinates the implementation of approved network configuration changes worldwide such as changes in network routing or numbering in the switches and changes in the IDNX/Promina configuration.

4.2.5 Operations and Maintenance Commands

The O&M Commands play a key role in the management of the DRSN. The O&Ms are directly responsible for the day-to-day operation of network switches, transmission facilities, and related equipment at individual DRSN switching sites. The O&Ms administer DRSN hardware and software, troubleshoot and repair equipment failures, reconfigure network assets in response to valid tasking, maintain configuration control over assets, and report local conditions that could affect network operations. The O&Ms also engineer, implement, and control features and functions at the end-user level (e.g., assignment and control of user instruments, features, and telephone numbers) and special site-specific sub networks that may share DRSN facilities such as SCAMPI, interfaces with tactical networks, and others. In addition to the functional requirements at the end-user level, it is suggested that O&Ms establish a proactive relationship with their customers, which fosters a smooth and effective troubleshooting process when responding to end-user problem calls. The O&Ms are also responsible for the overall security of their DRSN sites.

Figure 4-1 illustrates the network management data flow between the three levels of the DRSN hierarchy. Each link in the data flow is critical to the overall coordination, troubleshooting, and O&M activities needed to provide the end-user with high-quality service.

4.3 NETWORK MANAGEMENT POINT OF CONTACT NUMBERS

Table 4-1 provides POC numbers for the GNOSC and RNOSCs.

Table 4-1. Network Management POC Numbers

LOCATION	DSN NUMBER	COMMERCIAL NUMBER	FAX NUMBER
GNOSC-DOD DISA HQ Arlington, VA.	(312) 327-4034	(703) 607-4001/4002	DSN: (312) 607-4009
RNOSC-Scott AFB, IL.	(312) 779-9000 or (312) 779-9020 DRSN Secure: 80-631-6486 or 80-631-6487	(618) 229-9000 (618) 229-9020	DSN: (312) 779-9044
RNOSC-EUR (DISA-EUR) Vaihingen (Patch Barracks), GE.	(314) 430-6373 (314) 430-5955 (314) 430-6372	+49-711-680-6373/5955	DSN: (314) 430-4071
RNOSC-PAC (DISA-PAC) Wheeler Army Air Field, HI.	(315) 456-2777 (315) 456-2159	(808) 656-2777 (808) 656-2159	DSN: (315) 456-1277/9311 Secure: (315) 456-4500

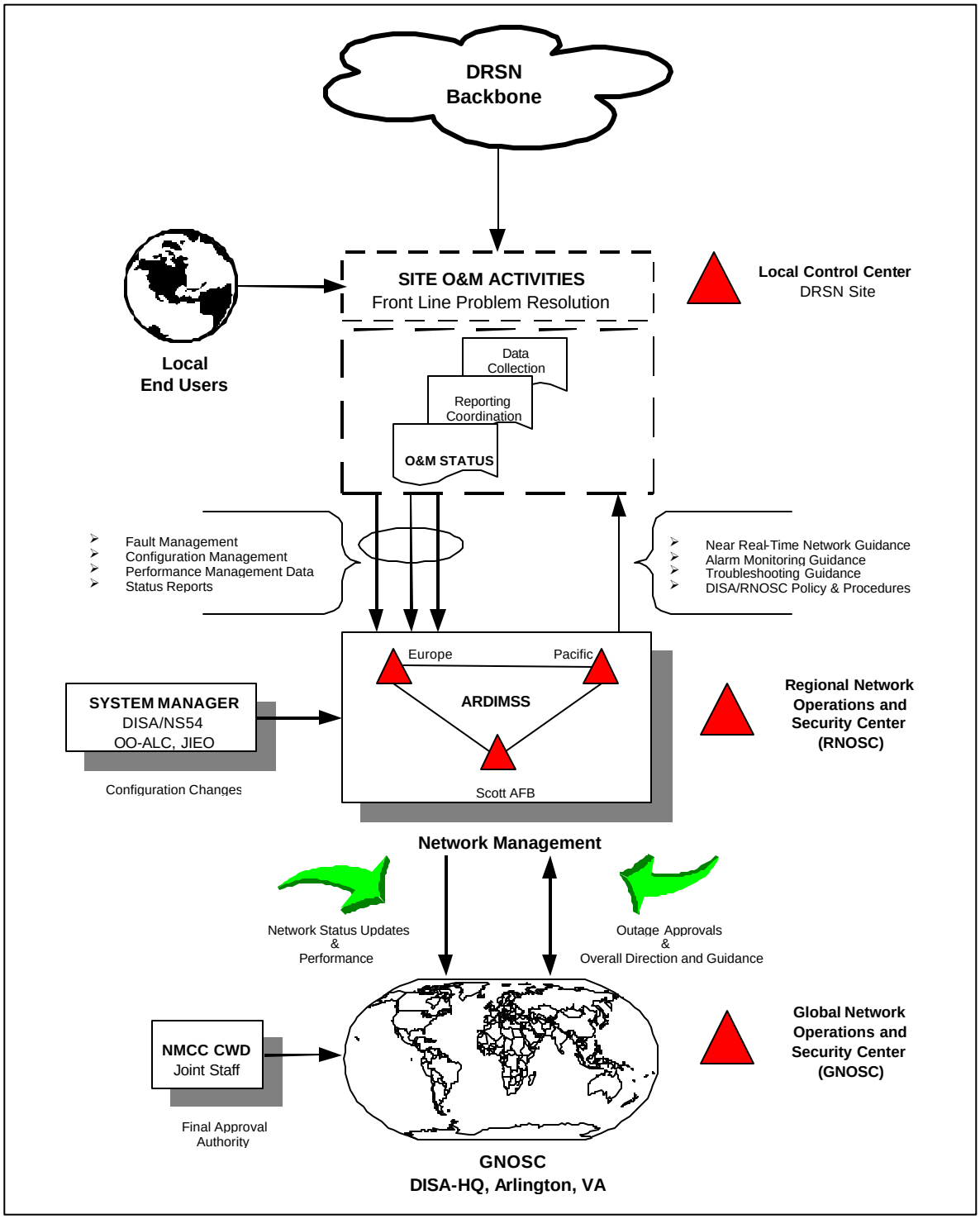

Figure 4-1. DRSN Network Management Communication, Guidance, and Data Flow

Intentionally left blank

PART II.
SITE ADMINISTRATION PROCEDURES

- Site Network Management Data Collection
- Site Security Management
- Ordering Telecommunications Service
- Site Record Keeping
  - Site Configuration
  - Maintenance
  - Inventory
- Access Instructions for Electronic Bulletin Board (EBB) System / Web Site

Intentionally left blank

SECTION 5
DRSN SITE NETWORK MANAGEMENT DATA COLLECTION

5.1 PURPOSE

This section identifies procedures for collecting and reporting DRSN data to support NM functions to include Performance Management, Configuration Management, Fault Management, Security Management, and Account Management.

5.2 DRSN DATA COLLECTION AND REPORTING PROCEDURES

The following series of tables provide suggested procedures for the O&Ms to use in supporting the DRSN NM data collection.

5.2.1 Fault Management Data Log

Each DRSN site must maintain a DRSN FM data log (see Table 5-1) in accordance with (IAW) DISA Circular (DISAC 310-70-1), DII Technical Control. The log can be maintained in a local database to support local O&M, Scott RNOSC troubleshooting, and FM efforts.

Table 5-1. Fault Management Data Log

WHAT	WHEN	WHO	HOW
Maintain a log of all user trouble reports and call failures in a local database.	Log all trouble reports and call failures as they occur or as they are reported.	Site O&M Personnel (Site Appointment)	IAW DISAC 310-70-1, record the following information: • Affected caller's SDN • Time problem occurred • Specific problem location • Nature of problem • Fix actions taken

NOTE: The document link below contains O&M information provided for replaceable items, preventive maintenance schedules and procedures, troubleshooting procedures, and repair information and procedures.

DSS-1 Digital Small Switch

5.2.2 Configuration Management and Performance Management Data Collection

Tables 5-2 through 5-5 provide step-by-step procedures for local data collection supporting network PM and CM. This data supports DISA's long-term network PM and CM processes of engineering, enhancing, and upgrading network topology. On a bimonthly basis, each site is required to send DISA Operational Management Section (NS54) their Call Detail History (CDH) and site User Identification Code (UIC) data. ***Note:*** The CDH procedures in Tables 5-2 and 5-3 have been updated with the Alpha processor. In addition, Tables 5-4 and 5-5 have been updated with Alpha processor procedures for collecting site UIC data.

To work within the DRSN security policies, DISA requires that each site collect the CDH data 30 days in advance of the UIC data. Each site will be responsible to hold the CDH data for 30 days. After 30 days, IAW DISAC 300-115-7, the CDH data and media will be declassified to For Official Use Only (FOUO) and mailed simultaneously (same tape or separate tapes) with the site UIC data. The site UIC data is classified SECRET. The entire package (both the CDH data and the UIC data) must be marked SECRET and mailed to DISA/NS54 per the schedules in the following tables.

5.2.2.1 Configuration Management Call Detail History Data Collection

Each DRSN site will provide switch CDH data IAW Table 5-2. The CDH data supports DISA's network CM process of controlling, auditing, and status accounting for all changes to the DRSN configuration baseline. Table 5-3 shows the procedures for the CDH data collection.

5.2.2.2 Performance Data Collection (User Identification Code)

Each DRSN site will provide switch UIC data IAW Table 5-4. This data supports DISA's network PM process. Table 5-5 shows the procedures for UIC data collection.

Table 5-2. Configuration Management CDH Data Collection

SUBSYSTEM	WHO	WHAT & WHEN	HOW
Switching CDH data collection will take place bimonthly to coincide with the site UIC data collection.	O&M Personnel (Site Appointment)	Provide site CDH for RED switches on a bimonthly basis to DISA/NS54. ***CDH DATA DATES*** 1-14 January 1-14 March 1-14 May 1-14 July 1-14 September 1-14 November ***TAPE PREPARATION DATES*** 14 January 14 March 14 May 14 July 14 September 14 November ***CDH DAT MAILING DATES*** (To be mailed with site UIC data) 15 February 15 April 15 June 15 August 15 October 15 December	See Call Detail History Data Collection Procedures, Table 5-3. The CDH data must be collected 30 days in advance of the site UIC data and held locally for 30 days as SECRET. After 30 days the CDH data will be downgraded to FOUO and mailed simultaneously with the site UIC data. Because the site UIC data is SECRET, package with both sets of data must be classified as SECRET when mailed to DISA/NS54.

Table 5-3. CDH Data Collection Procedures

This table contains the procedures for collecting call detail history of the Alpha processors. Because the SDS-1 switches use redundant processors, the call detail history can be divided between both processors. To ensure complete call detail history collection, perform the following procedures to merge the call detail history of the master processor with that of the standby processor.

A. At the DCL prompt, copy CDH files from the active processor to the standby processor.

B. To copy all CDH files, use the following command:
COPY *proc_name"user_idpassword*":SDS$CDHD:CDG*.* SDS$CDHD:*.*;2
where "proc_name" is the name of the off-line processor.

C. To copy a specific CDH file, use the following command:
COPY proc_name"user_idpassword":SDS$CDHD:CDHyyddd.extSDS$CMD:*.*.2

D. Start Call Detail utility by typing MANCDU<ENTER>. A menu is displayed.

E. Start the MERGE function by typing MERGE<ENTER>. If the user wishes to stop the MERGE function at any of the prompts specified in the following instructions, simply type EX<ENTER>. This will return the user to the MANCDU prompt.

F. Enter the extension for the files to process or press <ENTER> to accept the default file extension. The file extension can range in size from one to three characters.

G. Enter the Julian date of the beginning of the range of files that are to be merged. If only one day is to be merged, enter that date for both Julian date prompts.

H. Enter the Julian date of the ending of the range of files that are to be merged.

I. Insert the DAT tape into the standby processor.

J. Type: init mka500: cdh <ENTER>.

K. Type: backup/log dka300:[alphasds.100100]*.*:cdh.bck/save <ENTER>.

This operation copies all the CDH files to the tape. To read the tape to verify the copy process, do the following:

L. Type dismount mka500: <ENTER>.

M. Tape is ejected and must be reinserted.

N. Type back/list mka500: <ENTER>.

O. Type: dismount mka500: <ENTER>.

P. After preparing the RED CDH DAT, classify the tape at the SECRET level and forward to DISA/NS54.

Table 5-4. Performance Data Collection (UIC)

SUBSYSTEM	WHO	WHAT & WHEN	HOW
Switching	Site O&M Personnel (Site Appointment)	Provide site UIC data for RED switches bimonthly to DISA/NS54. Prepare the package cartridge (site UIC data) on the following dates: 15 February 15 April 15 June 15 August 15 October 15 December Mailing Address: DISA/NS54 11440 Isaac Newton Square Reston, VA 20190 The packaged cartridges will be promptly returned to each site immediately after processing.	See UIC Data Collection Procedures, Table 5-5. The site UIC data is not required to be held for 30 days. Site UIC data should be mailed at the same time as the CDH data (after the CDH data has been held locally for 30 days). The packaged cartridge with both sets of data must be classified SECRET and mailed to DISA/NS54.

Table 5-5. UIC Data Collection Procedures

UIC DATA COLLECTION PROCEDURES

This table contains the procedure to back up all files located in the site UIC of the processor. All entries are made at the associated console terminal (CRT) or X-Windows terminal. This procedure can also be used to perform weekly back-ups of the site UIC. Do not use this procedure to back up the entire hard disk. Total time for site UIC back up is approximately 2 to 3 minutes.

CAUTION

Database back-up procedures should be performed on the off-line processor ONLY. STOPSDS should be performed before doing back-up tapes, especially if deleting a directory.

NOTE

Step 2 in the following procedure may be omitted if the terminal is already logged on. If this is the case, ensure the terminal is at the root directory [XXXXXXXX] before proceeding.

1. Insert the DAT cartridge into the off-line Alpha processor. Wait until the green light on the tape drive stops flashing. A red light indicator on the front of the tape drive, with the tab inserted, indicates write protection is enabled. If indicator is lit, remove DAT and disable write protection. Reinsert DAT.

2. At the processor interface terminal (or CRT) or X-Windows terminal for the off-line processor, press the space bar to bring up the display. At the indicated prompts, enter the following commands:

   (a) Username: **XXXXXXXX [CR]**
   where XXXXXXXX is site-specific

   (b) Password: **YYYYYYYY [CR]**
   where YYYYYYYY is site-specific

3. If DAT cartridge is not initialized, initialize by entering:
   INIT MKA500: save_set [CR]
   where save_set is a maximum of six characters and is user defined. The save_set is used to identify a specific version to the tape (for example: save_set=JAN016).

4. At the prompt, type **ME [CR]** or **SITE [CR]** to get to the site UIC.

5. To begin back-up, at the prompt enter:

   BACKUP/LOG/VER DKA300:[ALPHASDS.SITE_UIC]*.* MKA500:save_set/SAVE[CR]

   (a) Where "**SITE_UIC**" is the name of the site UIC of the SDS-1.
   (b) "**save_set**" is the name used to identify the specific version of the tape provided in step c above.

   Defined switches are:
   /LOG Displays information about each file copied on the terminal.
   /VER Verifies each file is backed up correctly.

6. Remove DAT cartridge from the tape drive by pressing the eject button on the tape drive or entering:
   DISMOUNT MKA500: [CR].

7. When the data has been successfully captured, the operator will label the tape with the date, security classification of "SECRET," UIC directory, site location, POC, and POC DSN telephone number, and forward to DISA/NS54.

5.2.3 Security Data Management Requirements

Table 5-6 provides step-by-step procedures for local data collection-supporting network SM.

Table 5-6. Security Data Management Requirements

SUBSYSTEM	WHO	WHAT	HOW
RED and BLACK switches	Site O&M Personnel (Site Appointment)	Disable/Enable Codes	Train users on how to program telephones and the Group Enable/ Disable function. Ensure telephones are disabled when unattended.
		Switch Database Accounts. Change passwords periodically and anytime a user departs. Change passwords anytime they are included in data on DAT tapes.	Set up accounts for individuals needing access to the database and ensure the default login account (REDS) is deleted from the database.
		Maintenance Logs	Each switch will have a maintenance log to record all switch activity. The log will include date, time, name, and what activity.
		STU-III/R Keys	Call KMC at 1-800-635-6301 to rekey the STU-III/R keys annually.
		Facility Maintenance	All facility maintenance activities in the area of the switch will be done only in the presence of cleared switch maintenance personnel.

5.2.4 Accounting Data Management Requirements

Table 5-7 provides step-by-step procedures for local data collection-supporting network AM.

Table 5-7. Accounting Data Management Requirements

SUBSYSTEM	WHO	WHAT	HOW
RED and BLACK switches	Site O&M Personnel (Site Appointment)	Daily printout of the CDH files for the RED switch. Weekly printout of the CDH files for the BLACK switch. Maintain printed CDH files for 30 days.	Reports are printed on the off-line processor. Ensure printer is loaded with 132-column paper. Log in to the processor and enter CRT. After entering the REPORTS group, enter the DEMAND reports submenu. Enter the date of the CDH you wish to print out. Arrow over to Call Detail Record Report and enter "5" on the numeric keypad. If more reports are required, ensure the date is changed to reflect the report to be printed out.

5.2.5 RED Switch Level Device Reporting Requirement

Table 5-8 provides procedures for the "RED Switch Level Device" Reporting Requirement.

Table 5-8. RED Switch Level Device Reporting Requirement

SUBSYSTEM	WHO	WHAT	WHEN
RED Switches	Site O&M Personnel (Site Appointment)	To ensure timely and correct detection, notification, and repair of critical DRSN trunk and telephone instrument failures, it is imperative the Scott AFB Network Operation Center, along with the regional DISA operations centers, are updated when interface IDs (RCSSII) change (i.e., when general officers or VIPs move or change assignments, Permanent Change of Status (PCS) and/or RED instruments or trunks are added, deleted, or relocated).	RCSSII change reporting will be performed on an as required basis before implementation. At a minimum, sites will review master lists for accuracy on a quarterly basis.

All RED switch locations will maintain a master site list of all senior-level users, trunks, circuits or any other locally important devices. This master list will be updated when changes occur and transmitted to the Scott AFB Operations Center and theater centers if in DISA-PAC or DISA-EUR. All locations will check and update this information a minimum of quarterly to ensure accuracy. Table 5-9 provides an example of the master list format for reporting RCSSII updates.

Table 5-9. RED Switch Level Reportable Device Format

FULL NAME	RANK	TITLE	SDN	INTERFACE CARD TYPE	INTERFACE ID (RCSSII)	PORT	CCSD	DATA RATE	DISTANT END *
Jones, John J.	Gen	CINC AMC	1234	Quad Tele	120304567	02	- - - -	32 kb/s	- - - - - -
- - - - - -	- - - - -	- - - - - -	- - -	T1 Data	241501023	- - - - -	6U99	1.544 Mb/s	R04
* Note: "DISTANT END" is applicable to trunks only.									

Intentionally left blank

SECTION 6
DRSN SITE SECURITY MANAGEMENT

6.1 PURPOSE

This section addresses the DRSN day-to-day Security Management requirements. It identifies existing DRSN security directives and provides guidance for implementation of required security-related activities.

6.2 SECTION CONTENTS

Topics covered in this section are as follows:

- Responsibilities
- Accreditation and certification
- Access Measures
- Security Measures
- Information Classification
- Physical Measures

6.3 DEFINITIONS

Security management, threats, certification, and accreditation are explained in the following paragraphs.

6.3.1 Security Management

Each DRSN switch site must have a published system security plan (usually the Defense Intelligence Agency (DIA)-approved accreditation test report will suffice for the Sensitive Compartmented Information (SCI)-accredited nodes) that prescribes component configuration and procedures for:

- Safeguarding the switch complex
- Enforcing access controls to switch complex components
- Assigning subscriber terminal identifications and class markings
- Modifying the switch firmware and software

6.3.2 Threat

The DRSN is subject to many threats from a variety of sources. To maintain DRSN integrity, DRSN facilities (switches and associated equipment) must be protected from unauthorized modifications that could jeopardize network operations. Unauthorized manipulation of databases

or other software could result in a significant threat to command, control, and communications and the national security.

6.3.3 Certification

Certification is a technical determination that a system satisfies established standards for security and integrity. Qualified technical personnel must verify that the system satisfies established standards for:

- Physical security
- Personnel security
- Operational security
- Computer security
- Communications security

6.3.4 Accreditation

Accreditation is a Designated Approving Authority (DAA) declaration that the system provides acceptable security and integrity. A DAA bases this management decision on the certification documentation and other factors, such as requests for waivers. The DIA is the DAA for SCI nodes. All other nodes are accredited by the DISA DAA.

6.4 SECURITY MANAGEMENT RESPONSIBILITIES AND PROCEDURES

Tables 6-1 through 6-6 provide responsibilities and procedures for the O&Ms to use in conducting SM of the DRSN. The tables do not address all possible events that could occur, however, they do identify some key security measures required for the DRSN. Refer to MILDEP procedures or contact your responsible RNOSC for assistance on procedures not addressed within these tables.

Table 6-1. Site Security Management Responsibilities

WHO	WHAT
RED Switch O&M Command	Each RED switch O&M Command is responsible for appointing an ISSO before accreditation testing.
The ISSO will:	1. Assign a security compartment level and a terminal identifier to each DRSN terminal access line and switch cryptographic interface. The ISSO position will not be occupied by the SSO. 2. Implement the switch-node security plan. In that capacity, the ISSO controls the modification or replacement of system hardware, software, firmware, or database contents that affect systems security features and any other changes involving granting or removing SCI access to a subscriber terminal. Additionally, the ISSO will control installation or relocation of subscriber terminals. 3. Ensure report (magnetic, electronic, and printed reports) classification is IAW DISAC 300-115-7, Chapter 5.

Table 6-2. Certification and Accreditation

EVENT	WHO	WHAT & WHEN	HOW
Request to connect a switch to the DRSN	Site O&M organization commander	Request and obtain authorization from DISA DAA before connecting switch.	IAW DISAC 300-115-7, Chapter 6
DRSN switch node collateral accreditation (non-SCI)	Site O&M organization commander	Request and obtain authorization from DISA DAA.	IAW DISAC 300-115-7, Chapter 6
Node SCI Accreditation (Initial)	Site O&M organization commander	Request and obtain authorization from 497 IG.	IAW DISAC 300-115-7, Chapter 6
Node SCI Accreditation (1-year renewal)	Site O&M organization commander	Request and obtain authorization from 497 IG.	IAW DISAC 300-115-7, Chapter 6
All hardware, firmware, or software changes that alter DRSN security features	Site O&M organization commander	Base node ISSO and SSO notify DISA/NS54 and inform JCS, DIA, and NSA of changes.	IAW DISAC 300-115-7, Chapter 6

Table 6-3. Access Control Measures

EVENT	WHO	WHAT	HOW
Switch Database Update and Maintenance	ISSO or System Administrator	Implement configuration control and a password system to restrict access. ***Note:*** Single password entry will allow unrestricted access into the system.	IAW DISAC 300-115-7, Chapter 2
Request for access to physical area (switch consoles and subscriber terminals)	O&M personnel and users	Ensure that only authorized persons are permitted access to this equipment.	IAW DISAC 300-115-7, Chapter 4
Requests for access to RED switch operating information, control functions, and software	ISSO or System Administrator	Establish an audit trail with sufficient detail to reconstruct significant events.	IAW DISAC 300-115-7, Chapter 4
Request for console access	ISSO or System Administrator	Restrict access using a password system.	IAW DISAC 300-115-7, Chapter 4
Request for terminal access	ISSO or System Administrator	Restrict access using a password system.	IAW DISAC 300-115-7, Chapter 4
Voice mailbox access	ISSO or System Administrator	Restrict access using a password system.	IAW DISAC 300-115-7, Chapter 4
IDNX/Promina Access Level Control	DISA	1. Level 1 Access. Restrict access using the password system established by the Scott RNOSC or theater RNOSC. 2. Level 2 Access. Coordinate with the Scott RNOSC or theater RNOSC to request temporary level 2 or higher access when local assistance is needed to bring the IDNX/Promina node back on-line.	IAW DISAC 300-115-7, Chapter 4, and *DRSN IDNX Access Policy and Procedures* developed by the Scott RNOSC

Table 6-3. Access Control Measures (continued)

EVENT	WHO	WHAT	HOW
IDNX/Promina Access Control Administration	RNOSC System Administrators	Manage, maintain, control, and assign individual access accounts and passwords. Basic administrator responsibilities include establishing and maintaining IDNX/Promina access account names and passwords, coordinating and approving use of any temporary higher level accounts, maintaining a log-on account log for remote users requiring higher than level 1 access, monitoring the network for improper use of access accounts, and initiating actions required to prevent any potential network degradation as a result of improper use of access accounts.	IAW DODD 5210.73, Chapter 2

Table 6-4. Communication Security Measures (SAL Classmarks)

EVENT	WHO	WHAT	HOW
Security Compartment Assignments	ISSO	Assign SALs.	IAW DISAC 300-115-7, Chapter 3, Table 3-3
SCIF switches and subscriber terminals	ISSO	Assign SCI SALs, as appropriate.	IAW DISAC 300-115-7, Chapter 4
ISTs (non-SCI)	ISSO	Assign non-SCI SALs, as appropriate.	IAW DISAC 300-115-7, Chapter 4
ISTs SCI-accredited	ISSO	Assign SCI SALs, as appropriate.	IAW DISAC 300-115-7, Chapter 4
Cryptographic Interfaces (STU-III/R, etc.)	ISSO	Assign SALs that correspond to the classification level of the COMSEC key the interface uses.	IAW DISAC 300-115-7, Chapter 4
Telephone and console interfaces	ISSO	Assign fixed or variable SAL to each access line.	IAW DISAC 300-115-7, Chapter 4
U.S. controlled areas	ISSO	Assign US/FORN SALs to access lines serving all subscriber terminals accessible by foreign personnel.	IAW DISAC 300-115-7, Chapter 4
Foreign access areas	ISSO	Assign US/FORN SALs, as appropriate.	IAW DISAC 300-115-7, Chapter 4
IDNX/Promina ports connected to non-SCI switch trunks	RNOSC	Classmark “Encrypted Routing: Don’t Care.”	IAW DISAC 300-115-7, Chapter 3
IDNX/Promina ports connected to SCI-accredited switch trunks	RNOSC	Classmark “Encrypted Routing: Required.”	IAW DISAC 300-115-7, Chapter 3

Table 6-4. Communication Security Measures (SAL Classmarks) (continued)

EVENT	WHO	WHAT	HOW
IDNX/Promina trunk cards between SCI-accredited DRSN switch nodes	RNOSC	Classmark "Encrypted: YES" at each end.	IAW DISAC 300-115-7, Chapter 3
IDNX/Promina trunk cards between non-SCI DRSN switch nodes	RNOSC	Classmark "Encrypted: NO" at each end.	IAW DISAC 300-115-7, Chapter 3
Local security options	ISSO	Follow guidelines for security options: SALs used, SAL assignments, number of STU-III interfaces, voice recorders, nonsecure calling, and Allied users.	IAW DISAC 300-115-7, Chapter 4

Table 6-5. Information Security Measures Classification

EVENT	WHO	WHAT	HOW
Handling of DRSN information, documentation, correspondence, and files regardless of security classification	Switch node O&M personnel, ISSO	Follow guidance and procedures prescribed in DISAC 300-115-7.	IAW DISAC 300-115-7, Chapter 5, Classification Guidance

Table 6-6. Physical Security Measures

EVENT	WHO	WHAT	HOW
Enhance survivability and readiness	All DRSN facilities	Implement physical and procedural security measures, as applicable.	IAW DISAC 310-90-1. Also, see DODD 5210.73.

SECTION 7
ORDERING TELECOMMUNICATIONS SERVICE

7.1 PURPOSE

This section provides a reference of existing policies and procedures for ordering telecommunications service and requesting logistics support for DRSN equipment and parts.

7.2 DEFINITIONS

The TSR, the DRSN Telecommunications Certification Office (TCO), and the Telecommunications Service Order (TSO) are explained in the following paragraphs.

7.2.1 Telecommunications Service Request

A valid, approved, and funded telecommunications requirement prepared in accordance with the format in chapter 3 of the DISA Circular 310-130-1 and submitted to a DISA or DISA activities for fulfillment. TSR's may not be issued except by a specifically authorized TCO.

7.2.2 Telecommunications Certification Office

The activity designated by a Federal department or agency to certify to DISA (as a operating agency of the National Communications System) that a specified telecommunications service or facility is a validated, coordinated, and approved requirement of the department or agency, and that the department or agency is prepared to pay mutually acceptable costs involved in the fulfillment of the requirement.

The DRSN Program Office is the Designated TCO for all actions (i.e.. start, change or discontinue) involving the transmission part of the DRSN.

7.2.3 Telecommunications Service Order

The authorization from Headquarters DISA, a DISA area, or DISA TMSO to start, change, or discontinue circuits or trunks and to effect administrative changes.

7.2.4 Request For Service (RFS)

The document used to initially request telecommunications service, which is submitted by the requestor of the service to his designated TCO.

7.3 SERVICE ORDERING PROCEDURES

Table 7-1 provides procedures for the O&Ms to use in ordering service for DRSN users. The table does not address all possible events that could occur, however, it does identify the most

common events in the DRSN. Refer to MILDEP procedures or contact your responsible RNOSC for assistance on procedures not covered by this table.

Table 7-1 also identifies events that may require O&M element action to request and order service.

Table 7-1. Ordering New Service

EVENT	WHO	WHAT	HOW
1. User request for IMMEDIATE, PRIORITY, or ROUTINE local (nonnetwork) service 2. User requests for DPMs, DPAs, and DTAs to provide nonnetwork access to the connected switch	O&M element and MAJCOM or CINC	1. Submit RFSs and feeder TSRs to local telecommunications service ordering MAJCOM or CINC. 2. Local MAJCOM or CINC approves and submits TSRs to the respective MILDEP TCO for certification.	IAW DISAC 310-130-1, Chapter 3
1. User request for network access and/or FLASH or FLASH OVERRIDE service 2. User requests for DPMs, DPAs, and DTAs to provide network access	O&M element and MAJCOM or CINC	1. Submit RFSs and feeder TSRs to local telecommunications service ordering MAJCOM or CINC. 2. Local MAJCOM or CINC approves and submits MTF RFS to the J6T.	IAW CJCSI 6215.01, Enclosure D, para. 2.b (4) and Enclosure F ***Note:*** See the *Raytheon O&M Instructions Technical Manual*, Chapter 3, Figure 3-1 for a sample MTF.
Request for Long-Haul Services: DSN, Commercial, FTS access	O&M element and MAJCOM or CINC	Submit RFSs to the respective MILDEP TCO.	

Note: Information copies of above actions are to be forwarded to DRSN Program Management Office (DISA/NS54).

SECTION 8
DRSN SITE RECORD KEEPING CONFIGURATION MANAGEMENT INVENTORY AND MAINTENANCE

8.1 PURPOSE

The purpose of this section is to establish essential requirements for the day-to-day O&M record keeping at DRSN sites in support of CM, inventory control, and maintenance. This is intended to supplement rather than supersede existing MILDEP and local CM, logistics, and maintenance policies and procedures.

8.2 SECTION CONTENT

This section includes Table 8-1, which specifies actions and record keeping relating to configuration changes, inventory changes, or maintenance actions.

The generic site layout and circuit diagrams (Figures 8-1, 8-2, and 8-3) define the essential level of detail to be recorded at each DRSN site.

8.3 DRSN OPERATIONS AND MAINTENANCE RECORD KEEPING PROCEDURES

Table 8-1 provides procedures for the O&Ms to use as a guide for day-to-day record keeping. The table does not address all possible record keeping events, however, it does identify the most common events in the DRSN.

Table 8-1. Record Keeping

EVENT	WHO	WHAT	HOW
Completion of installation, deinstallation, or modification of network or tactical trunk	O&M Personnel (Site Appointment) ***Note:*** For DIA-accredited sites, this function is performed by the ISSO.	• Add, update, or delete SDN, interface, and board definitions in the switch database. • Modify site layout and circuit diagrams and equipment inventory records, as necessary.	• IAW the *Raytheon E-Systems O&M Instructions Technical Manual*, Section 6-5 • IAW the DISA essential requirements stated in Figures 8-1 through 8-3
Addition or deletion of FLASH and/or FLASH OVERRIDE subscribers	O&M Personnel (Site Appointment) ***Note:*** For DIA-accredited sites, this function is performed by the ISSO.	Upon Joint Staff approval, add or delete FLASH or FLASH OVERRIDE classmark to/from subscriber's SDN definition.	IAW the *Status Reporting for the DCS*, Section 6-5
NS54 with RNOSC assistance direction to modify switch database for routing, numbering (NNXs), or SAL changes	O&M Personnel (Site Appointment) ***Note:*** For DIA-accredited sites, this function is performed by the ISSO.	Upload new ROUVAL, DIGVAL, or SALVAL into switch database per RNOSC message request. Provide hard copy of changes made to the RNOSC once changes have been made.	IAW Raytheon O&M instruction manuals (specific documents unknown)
RNOSC direction to modify SDN, interface, or board definitions	O&M Personnel (Site Appointment) ***Note:*** For DIA-accredited sites, this function is performed by the ISSO.	Modify SDN, interface, or board definitions in the switch database.	IAW the *Raytheon E-Systems O&M Instructions Technical Manual*, Section 6-5
Removal of SDN from service	O&M Personnel (Site Appointment) ***Note:*** For DIA-accredited sites, this function is performed by the ISSO.	Remove SDN and corresponding interface entry from the SDN and interface definitions in the switch database.	IAW the *Raytheon E-Systems O&M Instructions Technical Manual*, Section 6-5
Subscriber number change requiring update of the *DRSN Telephone Directory*	O&M Personnel (Site Appointment) ***Note:*** For DIA-accredited sites, this function is performed by the ISSO.	Notify DISA/NS54 of the change.	By way of AUTODIN message or Electronic Bulletin Board
Equipment installation and deinstallation	TCF and Switch Technicians	Modify site layout and circuit diagrams and equipment inventory records, as necessary.	IAW local inventory practices and the DISA essential requirements stated in Figures 8-1 through 8-3

Table 8-1. Record Keeping (continued)

EVENT	WHO	WHAT	HOW
Completion of scheduled and unscheduled equipment maintenance	TCF and Switch Technicians	• Update maintenance records. • Modify site layout and circuit diagrams and equipment inventory records, as necessary.	IAW local maintenance practices and the DISA essential requirements stated in Figures 8-1 through 8-3

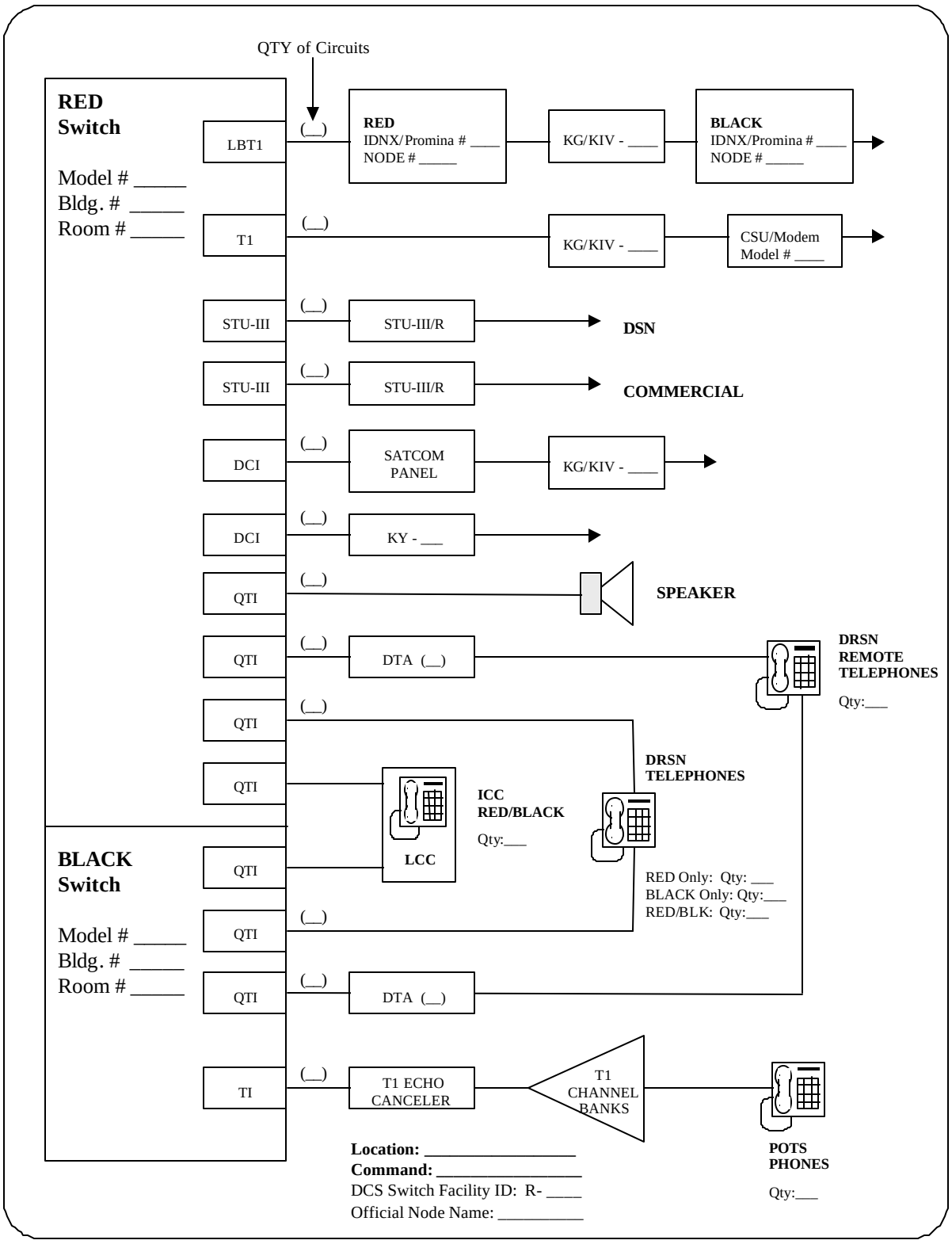

Figure 8-1. Sample Site Equipment Diagram

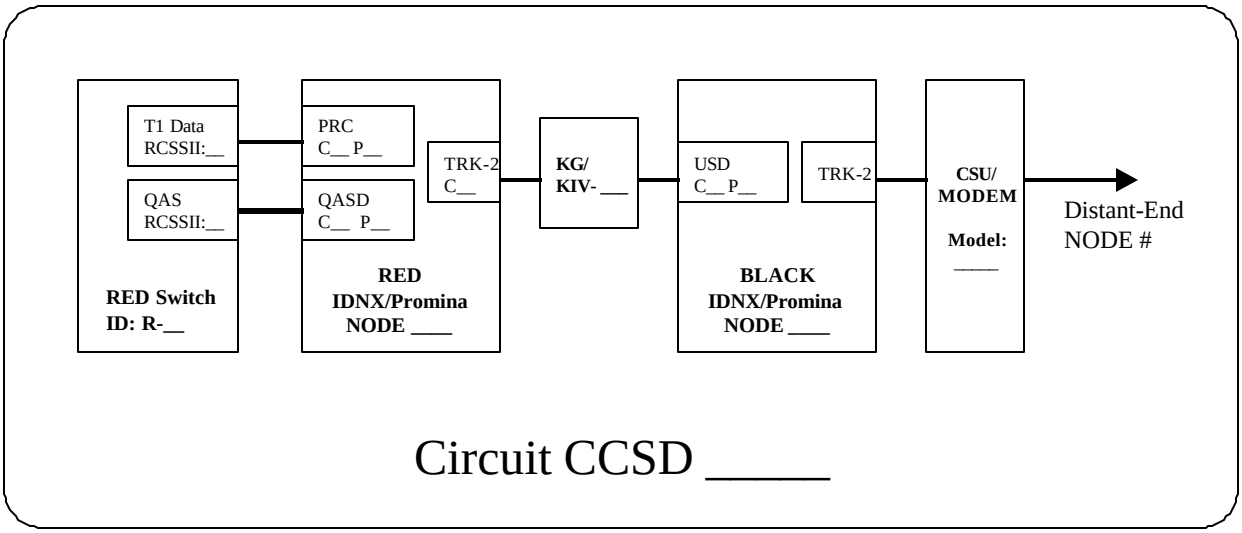

Figure 8-2. Sample Circuit Diagram

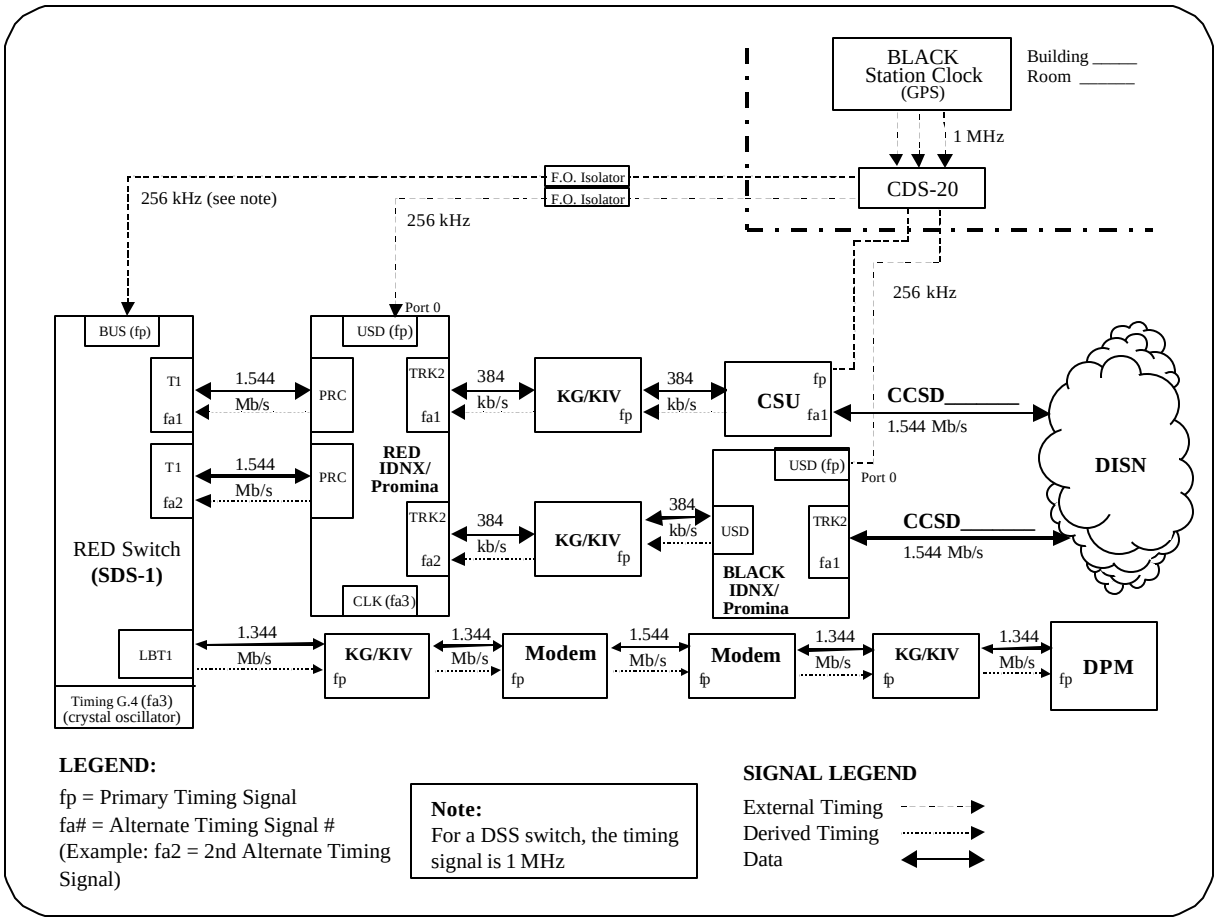

Figure 8-3. Sample T&S Diagram

Intentionally left blank

SECTION 9
DRSN ELECTRONIC BULLETIN BOARD SYSTEM

9.1 PURPOSE

This section provides procedures for accessing and registering on the DRSN EBBS. The EBBS is a communications tool provided to the DRSN community to communicate issues and concerns, lessons learned, policy and procedures, etc., in a real-time, day-to-day forum.

9.2 SECTION CONTENTS

Topics covered in this section are as follows:

- EBBS registration
- Access methods
- Registration example

9.3 ELECTRONIC BULLETIN BOARD SYSTEM REGISTRATION PROCESS

There are two ways to register for an EBBS account. The steps to register for the EBBS are as follows:

1. Access the DRSN EBBS WebPages described in paragraph 9.4.c. (http://drsnbbs.ncr.disa.mil)

2. Double click on "Installation Instructions" and then print the instructions out.

3. Double click on "Download Client Software."

4. Follow the installation instructions.

5. Once installed the New User Application is automatically sent to the System Administrator email account to await approval. To expedite validation of your account, contact the Administrator at DISA/NS54, (703) 735-8033 or DSN 653-8033.

OR

1. Access the DRSN EBBS using the method described in paragraph 9.4.a.

2. Double click on "Telnet Access to BBS."

3. Type “new” at the prompt and press [Return]. (example in Section 9.5)

4. Enter all the information requested. DO NOT leave any question blank. Enter “NA” if the question does not apply. We prefer that you use your first and last name as your UserID.

5. Following registration, your New User Application is automatically sent to the System Administrator email account to await approval. To expedite validation of your account, contact the Administrator at DISA/NS54, (703) 735-8033 or DSN 653-8033.

9.4 ELECTRONIC BULLETIN BOARD SYSTEM ACCESS METHODS AVAILABLE

Methods that are available for EBBS access are shown in the following:

a. EBBS Internet Access.

Telnet Connection:
IP Address: 164.117.160.224
Internet Name: drsnbbs.ncr.disa.mil
Communication Protocol: TCP/IP
Communication Emulations:

ASCII	ANSI	VT102/220

FTPs:

ASCII	XMODEM-Checksum	XMODEM-CRC
XMODEM-1K	YMODEM Batch	YMODEM-g
ZMODEM	ZMODEM (Resume after abort)	
Kermit /Super Kermit		

b. EBBS (Other Internet Access Methods).

FTP Connection:
Internet file transferring from BBS libraries using FTP.
ONLY REGISTERED USERS CAN ACCESS THE BBS THIS WAY, AND THIS METHOD ONLY ALLOWS DOWNLOADING AND UPLOADING OF FILES.

IP Address: 164.117.160.224
Internet Name: drsnbbs.ncr.disa.mil
Communication Protocol: TCP/IP

c. EBBS World Wide Web (WWW) Access.

WWW access is available using a Web browser like Mosaic, Netscape, etc. You can access the EBBS login instructions for FTP access from the browser, and other Government and commercial servers from the DRSN homepage.

IP Address: 164.117.160.224
Internet Name: drsnbbs.ncr.disa.mil

Open a URL or document (this is dependent on the browser being used) using either the IP address or name.

Example:
http://drsnbbs.ncr.disa.mil or http://164.117.160.224

9.5 REGISTRATION EXAMPLE

The following shows an example of how to register on the EBBS using telnet:

Auto-sensing.
WELCOME!

If you already have a User-ID on this system, type it in and press ENTER.
Otherwise type "new": ***new***

Welcome, newcomer! You have logged on to the world's most advanced multi-user online system: Worldgroup.

Before going into that, though, let's get acquainted. If you will tell us a little bit about yourself, we will create an account for you that you can use anytime for "free samples" of what we have to offer. There will be certain things you will not be able to do (like posting messages, etc.) until you elect to become a full Member of the Board. but you will have a chance to see if you like us first.

The following word may or may not be blinking: ANSI
Is it blinking (Y/N)? ***y or n***

Good! Your answer has been used to control the ANSI features of this system. Now if you will tell us a little about yourself, we will get underway.

Please enter your first and last name: ***John Doe***
Enter the first line of your address (your street address or P. O. Box): ***11440 Isaac Newton Sq.***
Enter the second line of your address (city, state, and ZIP): ***Reston, VA 20190***
Enter the last line of your address (Country or press ENTER for U.S.): ***USA***
Now enter the telephone number where you can be reached during the day: ***(703) 735-8033***
DSN Telephone Number: ***653-8033***

Now, you need to choose a "User-ID" for yourself. Your User-ID will be your "code name" on this system. You will use it to identify yourself to the system when you log on, and other users will know you by this name. Your User-ID can be 3 to 29 characters long (including letters, spaces, commas, periods, and hyphens). If you want it capitalized a certain way (for example, "John McLean"), type it in just that way. If you use all lower case, or ALL UPPER CASE, the system will apply its own capitalization standards.

Enter the User-ID you want to be known as: ***JohnDoe***

Here is a simulated message, showing how your User-ID will appear to other users:

From JohnDoe: How does this run so many users at once?

Are you satisfied with your choice of User-ID (y/n)? ***y***

Ok, JohnDoe, now you will also need to select a password, so that you can keep other people from using your account without your permission. Make it short and memorable, but not obvious. The security of your account depends on nobody else knowing what your password is.

Enter the password you plan to use: **********
Please reenter your password for verification: **********

WRITE YOUR INFORMATION DOWN, if you have not already. There will be nothing
anyone can do for you if you forget your User-ID or password. We do not give out people's passwords by mail or over the phone, even if they "sound" totally honest. Therefore, if you forget your password, or give it out to someone who should not have it, you are "up the creek." KEEP YOUR PASSWORD TO YOURSELF.

Press ENTER to create your account once you have written down your User-ID and password.
Welcome, then, to the DRSN BBS!

One moment, please…

Your application for an account on this system will now be reviewed.
One of our representatives will contact you shortly to confirm your status and arrange for validation of your account.

Thank you for calling!

PART III.
SITE O&M PROCEDURES

- Site Fault Management
- Site Preventative Maintenance
- Site Logistics and Repair Parts Support
- DRSN Management Database System

Intentionally left blank

SECTION 10
DRSN SITE FAULT MANAGEMENT

10.1 PURPOSE

This section identifies procedure references for O&M support of the day-to-day FM of the DRSN. Fault Management includes fault identification, troubleshooting, reporting, and correction.

10.2 SECTION CONTENTS

Topics covered in this section are as follows:

- Fault Identification
- Fault Troubleshooting
- Status Reporting
- Fault Correction

10.3 DEFINITIONS

Fault identification, troubleshooting, status reporting, and fault corrections are explained in the following paragraphs.

10.3.1 Fault Identification

Identification of faults is accomplished as follows:

- Local Identification. Local identification of faults is accomplished by the local O&M element through the monitoring of alarms, trouble reports, diagnostic tests, etc.

- Remote Identification. Remote identification of faults is accomplished through the Advanced DRSN Network Management System, using the ARDIMSS, IDNX/Promina Panvue and other NM tools.

10.3.2 Fault Troubleshooting

O&M network troubleshooting includes detecting and isolating abnormal network behavior. Some general O&M network troubleshooting tasks include:

- Examining error logs
- Troubleshooting alarms
- Tracing and identifying faults

- Performing diagnostic tests
- Reporting faults and corrections
- Performing call-through tests

10.3.3 Status Reporting

The DRSN reporting system is structured to provide operational information to DISA and the O&M Commands. The information is obtained through near-real-time nonformatted reports (current information) and daily formatted reports (historical information). These status reports enable the RNOSCs to exercise operational management control and conduct performance analysis of the network for quality improvement.

10.3.4 Fault Correction

Fault correction encompasses any or all actions taken to repair and restore one or more telecommunication services that have experienced a degraded quality of service or a service outage for any reason, including a damaged or impaired telecommunications facility.

10.4 DRSN FAULT MANAGEMENT PROCEDURES

Tables 10-1 through 10-8 provide procedures for the O&Ms to use for FM of the DRSN. The tables do not address all possible events that could occur, however, they do identify the most common problems encountered in the network. Refer to MILDEP procedures or contact your responsible RNOSC for assistance on procedures not covered by these tables. The following tables include:

- Unscheduled Service Interruptions and Outages (Table 10-1)
- Responding to Senior User Call Failures (Table 10-2)
- Switching Subsystem Alarm Events (Table 10-3)
- Transmission Subsystem Alarm Events (Table 10-4)
- Timing and Synchronization Subsystem Alarm Events (Table 10-5)
- Authorized Outages (Table 10-6)
- Authorized Outage Request Format (Table 10-7)
- Site Level Reporting Requirements (Table 10-8)

Table 10-1. Unscheduled Service Interruptions and Outages

EVENT (S)	WHO	WHAT & WHEN	HOW
DRSN Interswitch Trunk failure and associated equipment: • IDNX/Promina Hardware Failures • CSU Failure • KG Failure	O&M personnel and TCF at the location where the trunk failure is observed (Site appointment)	1. Immediately contact the RNOSC by telephone to open a trouble ticket for any trunk failure 10 minutes or longer. Document the following information as soon as possible: a. The time the problem occurred. b. Name and title of all users and callers affected, locations, instruments used, and switch interface IDs for instruments. c. Specific description of problem (include symptoms experienced by users, e.g., no audio, burst of noise for 15 seconds, etc.). d. For senior user issues, provide POCs and phone numbers of the user's communications support staff personnel with firsthand knowledge of the problems the user experienced. e. Fix actions taken to resolve the problem.	1. IAW DISAC 310-55-1, and DISAC 310-70-84, Chapter 3
		2. The TCF will begin prompt site-level troubleshooting. Provide periodic status updates to the RNOSC at least once per hour during troubleshooting.	2. IAW DISAC 310-70-1
		3. Restore service.	3. IAW DISAC 310-70-84, Chapter 4
		4. Perform call-through tests.	4. IAW DISAC 310-70-84, Chapter 4
		5. Notify the RNOSC of the completed fix action.	
		6. Coordinate with the RNOSC before beginning any troubleshooting on DRSN transmission paths.	

Table 10-1. Unscheduled Service Interruptions and Outages (continued)

EVENT (S)	WHO	WHAT & WHEN	HOW
DRSN switching or processor failure	O&M technician at failed equipment location	1. Contact the RNOSC by telephone to open a trouble ticket for any facility outage or failure 1 minute or longer. Document the following information as soon as possible: a. The time the problem occurred. b. Name and title of all users and callers affected, locations, instruments used, and switch interface IDs for instruments. c. Specific description of problem (include symptoms experienced by users, e.g., no audio, burst of noise for 15 seconds, etc.). d. For senior user issues, provide POCs and phone numbers of the user's communications support staff personnel with firsthand knowledge of the problems the user experienced. e. Fix actions taken to resolve the problem. 2. Begin troubleshooting. Provide periodic status updates to the RNOSC at least once per hour during troubleshooting. 3. Restore service. 4. Perform call-through tests. 5. Notify the RNOSC of the completed fix action.	1. IAW DISAC 310-55-1, and DISAC 310-70-84, Chapter 3 2. IAW DISAC 310-70-1 3. IAW DISAC 310-70-84, Chapter 4 4. IAW DISAC 310-70-84, Chapter 4

Table 10-2. Responding to Senior User Call Failures

EVENT	WHO	WHAT & WHEN	HOW
Senior level user circuit failure or trouble report (Senior users are defined as general officers or senior executive service civil servants.)	RNOSC and O&M element that received the trouble report or complaint	1. Immediately contact the respective RNOSC by telephone to open a trouble ticket for any senior user call failure. Provide POCs and telephone numbers of the user's communications support staff personnel with firsthand knowledge of the problems the user experienced. 2. Begin prompt site-level troubleshooting. Provide periodic status updates to the RNOSC at least once per hour during troubleshooting. 3. Restore service and perform call-through tests. 4. Coordinate, confirm, and document the final fix action with the RNOSC. 5. Coordinate with the RNOSC before beginning any troubleshooting on DRSN transmission paths.	1. Provide the following to the RNOSC: a. Affected caller(s) SDN b. When the problem occurred c. Where the problem occurred, include specific location, e.g., office, operations position, residence, etc. d. Nature of problem; provide specifics 2. Fix action, includes all site-level actions taken to troubleshoot and resolve the problem

Table 10-3. Switching Subsystem Alarm Events

EVENT	WHO	WHAT	HOW
ARDIMSS observed switch alarms that are or may potentially affect network service	RNOSC and switch technicians	1. RNOSC contacts site. 2. Site follows step-by-step procedures as directed by the RNOSC. 3. Switch technicians call the RNOSC to report correction of the fault.	IAW RNOSC directed policy and procedures
Locally observed alarms that affect or may potentially affect network service	Switch technicians	1. Contact the RNOSC by telephone to indicate the nature of the problem. 2. Follow locally established troubleshooting procedures. 3. Restore service and/or correct alarm problems. 4. Perform call-through tests. 5. Report fix actions to the RNOSC upon restoral.	IAW RNOSC policy and procedures and Raytheon O&M manuals

Table 10-4. Transmission Subsystem Alarm Events

EVENT	WHO	WHAT	HOW
IDNX/Promina alarms indicating a faulty component	O&M personnel and switch technicians	1. Contact the RNOSC. 2. Isolate the fault in cooperation with the RNOSC. 3. Provide the RNOSC with the following information to ensure replacement parts are properly shipped: a. Location and affected node number b. Major end item the faulty component is part of c. Revision number, if applicable d. Quantity needed e. Complete mailing or shipping address	IAW IDNX/Promina maintenance procedures established by the Scott RNOSC. ***Note:*** In cases where it is not possible to wait for the next duty day, the RNOSC will work with N.E.T.'s` technical assistance center to arrange for shipment sooner. Special Maintenance Problems: When a problem is beyond the capabilities of the site maintenance personnel or the RNOSC controllers to troubleshoot or correct, the RNOSC will arrange for on-site technical assistance.
CSU alarms	O&M personnel responsible for FM of CSU equipment	1. Isolate the problem at the faulty CSU. 2. Replace the faulty CSU. 3. Perform call-through tests.	IAW local CSU troubleshooting policies
CRYPTO alarms	O&M and TCF personnel responsible for FM and correction of KG equipment and circuit faults	1. O&M personnel contact the RNOSC to report the fault and obtain a trouble ticket. 2. Begin standard crypto troubleshooting practices. 3. Perform call-through tests. 4. O&M personnel to contact the RNOSC upon correction of the KG fault.	IAW local crypto troubleshooting policies

Table 10-5. Timing and Synchronization Subsystem Alarm Events

EVENT	WHO	WHAT	HOW
Timing slips and loss of synchronization	TCF	Troubleshoot for LBCI, jitter, clock failures, etc.	IAW DISAC 310-70-1, Chapter 4, para. 7 and Supplement 1, Chapter 24 (Digital Jitter Testing)

Table 10-6. Authorized Outages

EVENT	WHO	WHAT & WHEN	HOW
Scheduled outage for the following: a. DRSN IST b. Tail Segment c. DRSN switches d. DRSN IDNX/Promina e. Partial Facility Outages f. Complete Facility Outage g. DPA/DPM Outages (see ***Note:*** 1 in the "How" column of this table) h. Power or UPS	Local DRSN O&M personnel responsible for each subsystem	1. Obtain user release, including affected CINCs, MAJCOM command centers, and other supported units, before requesting a scheduled service interruption through the RNOSC. 2. Schedule and plan service interruptions with the RNOSC by message 14 days in advance of desired A/O date to maximize communications capabilities. See A/O request format in Table 10-7. 3. Obtain final approval from the RNOSC 30 minutes before the interruption IAW the *Joint Logistics Support Plan (SP)*, Chapter 7, para. 3f. 4. Notify the RNOSC of the restoral of service.	IAW DISAC 310-70-1, Chapter 7, para. 3, and DISAC 310-70-84, Chapter 3. ***Note:*** 1: O&M elements must request and coordinate with the RNOSC 24 hours in advance of any DPM/DPA A/Os affecting service to senior level users: a. NCA or military service chiefs b. Unified commanders c. MAJCOM commanders d. WWSVCS or AF Four-star conferees
Waivers	RNOSC	Some contingencies or emergency situations may justify waiving standard requesting submission and notification times. On a case-by-case basis, the RNOSC may request and coordinate expedited approval of A/Os to support maintaining effective network services.	IAW with respective RNOSC policy and procedures

Table 10-7. Authorized Outage Request Format

ITEM	DESCRIPTION
1.	Date and Time. Provide primary date, alternate date, and inclusive times (and alternate times) of the scheduled interruption. If the A/O must occur during peak traffic periods (on normal duty days between 1000Z and 2200Z) include justification.
2.	Purpose. Provide an explanation fully describing the purpose of the A/O.
3.	Alternatives. Provide a statement confirming that other alternatives (other than needing a complete switch downtime or isolation) have been considered and are not practical or possible.
4.	Work POCs. Identify the personnel responsible for completing actions planned during the A/O (include name, telephone number, e-mail address, and military organization or office symbol or civilian contractor organization).
5.	Materials. Provide a statement confirming that all required parts and equipment are on-hand to complete the A/O actions or identify the expected delivery date of materials on order.
6.	Recovery. Identify the estimated recovery time once the scheduled service interruption starts.
7.	User Release. Identify users and state concurrence of local users with the dates and times of the requested service interruption. When it is not possible to obtain required release from all users and the A/O request cannot be delayed, provide a list of the users that have not yet concurred.
8.	A/O Project Officer. Identify the name, telephone number, and e-mail address of the primary and alternate project officer for the scheduled outage.
9.	Processing. GNOSC, RNOSC, and NMCC CWD, and Joint Staff processing, coordination, and approval. RNOSC notifies the site of NMCC CWD approval.
10.	Final Approval. Site confirms approval of scheduled service interruption with the RNOSC 30 minutes before the start of the A/O.

Table 10-8. Site Level Reporting Requirements

REPORTABLE EVENT	WHO	WHAT & WHEN	HOW
• Trunk failures with a duration of 10 minutes or longer • Circuit failure, including remote DPA/DTA interfaces (senior users) • Switching or processor failure (1 minute or longer) • Switching system isolation (1 minute or longer) • IDNX/Promina hardware failures • CSU failure • HAZCONs (30 minutes or longer)	TCF and switch technician	1. Immediately contact the RNOSC by telephone to open a trouble ticket. Document the following information as soon as possible: a. The time the problem occurred. b. Name and title of all users and callers affected, locations, instruments used, and switch interface IDs for instruments. c. Specific description of problem (include symptoms experienced by users, e.g., no audio, burst of noise for 15 seconds, etc.). d. For senior user issues, provide POCs and phone numbers of the user's communications support staff personnel with firsthand knowledge of the problems the user experienced. e. Fix actions taken to resolve the problem. f. Provide periodic status update to the RNOSC or Scott RNOSC (at least every hour) during troubleshooting. g. Confirm and document the RFO with the RNOSC or Scott RNOSC after the problem is resolved; coordinate and document the time of the confirmation with the RNOSC or Scott RNOSC. h. Coordinate, confirm, and document the final fix action with the RNOSC; coordinate and document the time of the confirmation with the RNOSC.	IAW DISAC 310-70-84, Chapter 3.

Intentionally left blank

SECTION 11
DRSN SITE PREVENTIVE MAINTENANCE

11.1 PURPOSE

To effectively maintain reliable and satisfactory network performance, this section prescribes procedures that constitute the minimum SWITCH preventive maintenance guidelines for all DRSN sites.

11.2 SECTION CONTENTS

Topics covered in this section are as follows:

- Periods of performance
- Daily Maintenance Inspections (Table 11-1)
- Weekly Maintenance Inspections (Table 11-2)
- Monthly Maintenance Inspections (Table 11-3)
- Quarterly Maintenance Inspections (Table 11-4)
- Annual Maintenance Inspection (Table 11-5)
- Other Tape Back-Ups (Table 11-6)
- Crypto Change-Out and Rekey Procedures (Table 11-6)
- Updating the KG-94/94A Traffic Encryption Key (TEK) through Change Key Operation (Table 11-7)
- Procedures to Load KEYMAT into the KIV-7/HS (Table 11-8)
- Procedures to Update Keys in the KIV-7/HS (Table 11-9)
- Procedures to TX a Key Stored in the KIV-7/HS to Distant-End (Table 11-10)
- Procedures to Zeroize Keys in the KIV-7/HS (Table 11-11)
- Procedures to Select a Key for Operation in the KIV-7/HS (Table 12-13)

11.3 DRSN OPERATIONS AND MAINTENANCE PREVENTIVE MAINTENANCE PROCEDURES

DRSN O&M preventive maintenance inspections performed on a daily, weekly, monthly, and quarterly basis are detailed below.

11.3.1 Periods of Performance

Sites will coordinate with their respective RNOSC ***before*** conducting any maintenance actions that place a switch in a hazardous condition (i.e., during performance of the maintenance action). This helps to minimize the risk of degrading service to network customers, especially during prime operational hours.

A few inspections and system back-up procedures hard disk software back-up tape/System Configurations need dedicated use of one of the two switch processors – leaving the on-line processor without an available hot back up. Sites should plan to complete procedures of this nature during nonprime service hours.

Table 11-1. Daily Maintenance Inspections

INSPECTION ITEM	WHO	WHAT	HOW
Printer Monitoring	O&M Personnel (Site Appointment)	Check printer messages routinely. Always review messages printed during any unattended periods. Ensure both processors report "NO ALARMS." When alarms occur, use locally established procedures to identify the source, correct the problem(s), and clear the alarms. Immediately report all alarms related to service failures and HAZCONs to the appropriate RNOSC.	IAW with locally established procedures.
Out-dial Capability	O&M Personnel (Site Appointment)	Confirm out-dial capabilities by making calls over each T1 and/or ancillary trunk associated with the switch system. Test tones from distant-end switches will suffice if site DIGVAL tables and trunk classmarks support this maintenance-initiated feature.	IAW with locally established procedures.

Table 11-1. Daily Maintenance Inspections (continued)

INSPECTION ITEM	WHO	WHAT	HOW
Subscriber Calling Capability	O&M Personnel (Site Appointment)	For critical subscribers, a test call will be made to the RNOSC-EUR, RNOSC-PAC, or Scott RNOSC to verify that required functionality is available.	IAW with locally established procedures.
System Configurations	O&M Personnel (Site Appointment)	Rotate processor/timing every week to verify operation and redundancy with all processor/timing system configurations. Model Rotation Schedule: Week 1: APROC/A Timing Week 2: APROC/B Timing Week 3: BPROC/B Timing Week 4: BPROC/A Timing Week 5: APROC/A Timing Rotation begins again.	***Note:*** This procedure will be performed during nonprime service hours. Before performing this procedure first, ensure that no users are currently on-line.

Table 11-2. Weekly Maintenance Inspections

INSPECTION ITEM	WHO	WHAT	NOTES AND EXAMPLES
Memory and Disk Management	Site Appointment, Switch Technicians ***Note:*** This is usually a CSO function.	Monitor memory use and disk space availability. Purge old, redundant, and/or outdated system files to ensure maximum amount of disk space. Periodically, clear switch log and net log files from the database used to print or store error messages (particularly important on DSS systems because of the limited disk space).	Field Bulletin FB 178 SDS Alpha directs clocks.
System Configurations	O&M Personnel (Site Appointment)	Rotate processor/timing every week to verify operation and redundancy with all processor/timing system configurations. Model Rotation Schedule: Week 1: APROC/A Timing Week 2: APROC/B Timing Week 3: BPROC/B Timing Week 4: BPROC/A Timing Week 5: APROC/A Timing Rotation begins again.	***Note:*** This procedure will be performed during nonprime service hours. Before performing this procedure first, ensure that no users are currently on-line.
Site UIC Processor Files	O&M Personnel (Site Appointment)	Make back-up tapes of site-unique files. Maintain all tapes in a separate location. Alternately make one site UIC tape for each system or processor and update the tapes every other week. Do the same for console database.	***Note:*** A UIC must be purged before making a back up. Example: Week 1: Make a new "A" Proc site UIC tape. Week 2: Make a new "B" Proc site UIC tape. Week 3: Update the "A" tape. Week 4: Update the "B" tape. The cycle repeats.
Processor Cabinet and Switch Blower Motors	Switch Technicians	Check and ensure all blowers are operational and airflow is unobstructed.	
DTMF, Registers	Switch Technicians	Confirm operation by maintenance initiated test or by monitoring incoming calls to ensure each interface is selected and responds correctly.	
Tone Generator	Switch Technicians	Verify operation by maintenance initiated test or by monitoring outgoing calls to ensure each interface is selected and responds correctly.	
Announcers	Switch Technicians	Verify proper operation.	

Filters	Switch Technicians	Change all equipment filters. Check and ensure all air outlets and intakes around the switch are clear.	***Note:*** Sites should maintain a spare set of filters for all equipment.

Table 11-3. Monthly Maintenance Inspections

INSPECTION ITEM	WHO	WHAT	NOTES AND EXAMPLES
Switch Processor Clock Checks		To ensure accurate and synchronized reporting of alarm times by switches throughout the DRSN, perform the following procedure once a month for each switch processor: a. Time. Using the terminal, type "SET TIME," then enter the correct time in the format "HR:MM:SS," and follow with a carriage return (<CR>). Sample: SET TIME 08:05:22 <CR>. b. Time and Date. If the date also needs correction, after typing "SET TIME," enter the date in the format "DD-MM-YY," insert a space (<SPACE>), enter the time "HR:MM:SS," and then follow with <CR>. Sample: SET TIME 01-01-94 <SPACE>08:05:22<CR>.	***Note*** 1: After performing the clock check procedure, the system responds with a prompt. After the prompt, type "show time" and follow with a <CR>. ***Note*** 2: The procedure must be completed individually for each processor, since the processors do not transfer time updates through the interprocessor link.

11.3.2 Quarterly Maintenance Inspection

Coordinate quarterly maintenance inspections with the Scott RNOSC.

Table 11-4. Quarterly Maintenance Inspection

INSPECTION ITEM	WHO	WHAT	NOTES AND EXAMPLES
Card Cage +5VDC, +/-12VDC, -48VDC, and +5VDC Bus Isolation Diode Checks	Site Appointment, Switch Technicians	Verify voltage levels at the card cage level. Follow technical manual information and/or local preventive maintenance instructions for voltage adjustments and power supply tests.	This procedure will be performed more often if needed by the equipment environment.
Switch Cabinet Power Supply Voltage Checks	Site Appointment, Switch Technicians	Verify voltage levels of the switch cabinet power supply.	This procedure will be performed more often if needed by the equipment environment.

Table 11-5. Annual Maintenance Inspection

INSPECTION ITEM	WHO	WHAT	NOTES AND EXAMPLES
Switch Cabinets	Site Appointment, Switch Technicians	Corrosion Control	This procedure will be performed more often if needed by the equipment environment.

11.3.3 Other Tape Back-ups

Coordinate tape back-ups with the Scott RNOSC. In addition to those previously identified, sites must also maintain back-ups of a number of other tapes as described in Table 11-6. O&M personnel responsible for DRSN switch systems should include System Backup/Restoral Procedures as mandatory actions in locally developed preventive maintenance operating instructions, procedures, and checklists. Please contact the Scott RNOSC technicians at DSN 779-9020, if you need any help with completing the procedures described below.

System Backup/Restoral Procedures Using the Version 14 Installation/Maintenance Media

The steps outlined below are for use with the Raytheon provided Version 14 lnsta1Iation~ Maintenance CD-ROM. This procedure is provided to facilitate the Backup/Restoral process of the system hard disk. This procedure is NOT contained in the Operations and Maintenance Manual for the switch.

NOTE: All of the steps outlined below must be performed from the CRT/ Maintenance terminal.

Backup of the System Hard Disk

1. Hard lock the Control/Status Panel to the on-line processor.

2. Log on to the off-line processor as ALPHASDS, password SDSALPHA or equivalent.

3. Enter **STOPSDS <enter>.**

4. Log out of the processor and back in as SYSTEM, password PROCESSORA or PROCESSORB, depending on which processor you are logging into.

5. Type **SHUTDOWN <enter>.**

6. Plug the CD-ROM drive in to the back of the Alpha processor and apply power to the drive.

7. Insert the “Version 14 Installation/Maintenance Media” CD-ROM in to the drive.

8. At the >>> prompt, type **BOOT DKB500: <enter>.**

9. The main menu will reappear as shown:

****

This CD-ROM can permit you to perform the following:

- o Install the OpenVMS 7.1 Operating System
- o Install the SDS V14 Calls Software
- o Install the SDS LCC-l V2 Software

You can also execute DCL commands and procedures to perform "standalone" tasks, such as backing up the system disk.

Please choose one of the following:

1) Install the OpenVMS 7.1 Operating System
2) Process the Site UIC
3) Install the SDS V14 Calls Software
4) Install the SDS LCC-1 V2 Software
5) Backup the system hard disk to tape
6) Restore the system hard disk from tape
7) Execute DCL commands and procedures
8) Shut down this system

Enter CHOICE or ? for help: (l/2/3/4/5/6/7/8/?)

Type 5 <**enter>.**

10. The following will appear:

Please enter a 1 to 6 character name for the backup tape label (do not use spaces or special characters in the label):

Enter a six character or less label for the backup tape. Use only alphabetic or numeric characters. You may use hyphens (-) and underlines (_) in the label. Press **<enter>**

11. The following will appear:

Insert a 4mm DAT tape into the tape drive. Verify that the tape is not write protected.

WARNING: All data currently on the tape will be destroyed. Do you wish to Continue with the backup process (Yes/No)? [N]

If you are ready to backup the hard disk, enter **Y <enter>.** If you would like to abort the

process and return to the main menu, press **<enter>**

12. After the backup is complete, press **<enter>** to be returned to the main menu.

13. The following will appear:

****

This CD-ROM can permit you to perform the following:

- o Install the OpenVMS 7.1 operating System
- o Install the SDS Vl4 Calls Software
- o Install the SDS LCC-l V2 Software

You can also execute DCL commands and procedures to perform "standalone" tasks, such as backing up the system disk

Please choose one of the following:

1) Install the OpenVMS 7.1 Operating System
2) Process the Site UIC
3) Install the SDS V14 Calls Software
4) Install the SDS LCC-l V2 Software
5) Backup the system hard disk to tape
6) Restore the system hard disk from tape
7) Execute DCL commands and procedures
8) Shut down this system

Enter CHOICE or ? for help: (l/2/3/4/5/6/7/8/?)

Enter **8 <enter>** to shutdown the system.

14. Once the system has shutdown, and the >>> prompt has returned, power off the Alpha processor and disconnect the CD-ROM drive from the Alpha processor.

15. Power the Alpha processor back up.

16. Verify the Alpha processor boots correctly and start calls processing.

17. Disconnect the CRT cable from the back of the Alpha processor.

Restoral of the System Hard Disk

If the processor is currently up and operational, proceed with the following procedure at Step 1. If this is a replacement of the system hard disk, it is assumed that the processor is already at a ">>>" prompt and you should begin with this procedure at Step 6.

1. Hard lock the Control *I* Status Panel to the on-line processor.

2. Log on to the off-line processor as ALPHASDS, password SDSALPHA or equivalent.

3. Enter **STOPSDS <enter>.**

4. Log out of the processor and back in as SYSTEM, password PROCESSORA or PROCESSORB, depending on which processor you are logging into.

5. Type **SHUTDOWN <enter>**

6. Plug the CD-ROM drive in to the back of the Alpha processor and apply power to the drive.

7. Insert the "Version 14 Installation/Maintenance Media" CD-ROM in to the drive.

8. At the >>> prompt, type **BOOT DKB500: <enter>**

9. The main menu will reappear as shown:

****

This CD-ROM can permit you to perform the following:

- o Install the OpenVMS 7.1 operating System
- o Install the SDS Vl4 Calls Software
- o Install the SDS LCC-l V2 Software

You can also execute DCL commands and procedures to perform “standalone” tasks, such as backing up the system disk

Please choose one of the following:

1) Install the OpenVMS 7.1 Operating System
2) Process the Site UIC
3) Install the SDS V14 Calls Software
4) Install the SDS LCC-l V2 Software
5) Backup the system hard disk to tape
6) Restore the system hard disk from tape
7) Execute DCL commands and procedures
8) Shut down this system

Enter CHOICE or ? for help: (l/2/3/4/5/6/7/8/?)

Type 6 **<enter>.**

10. The following will appear:

This procedure will restore the system hard disk from tape. This procedure will ONLY restore to the hard disk set as DKA300:. If you wish to restore the 535MB hard disk (DKA100:), you must exit this and use the commands in the operations and Maintenance Manual.

Please enter the 1 to 6 character name of the backup tape label (the name you enter MUST match exactly what was entered when the tape was made)

Enter the six character or less label for the backup tape. Use only alphabetic or numeric characters. You may use hyphens (-) and underlines (_) in the label. Press **<enter>**

11. The following will appear:

Insert the 4mm DAT tape into the tape drive. Verify that the tape is write protected.

> **WARNING**: All data currently on the target hard disk will be destroyed do you wish to continue with the restore process (Yes/No)? [N]

If you are ready to restore the hard disk, enter **Y <enter>.** If you would like to abort the process and return to the main menu. press **<enter>**

12. After the backup is complete, press **<enter>** to be returned to the main menu.

13. The following will appear:

****

> This CD-ROM can permit you to perform the following:
>
> - Install the OpenVMS 7.1 operating System
> - Install the SDS Vl4 Calls Software
> - Install the SDS LCC-l V2 Software
>
> You can also execute DCL commands and procedures to perform “standalone” tasks, such as backing up the system disk
>
> Please choose one of the following:
>
> 1) Install the OpenVMS 7.1 Operating System
> 2) Process the Site UIC
> 3) Install the SDS V14 Calls Software
> 4) Install the SDS LCC-l V2 Software
> 5) Backup the system hard disk to tape
> 6) Restore the system hard disk from tape
> 7) Execute DCL commands and procedures
> 8) Shut down this system

Enter CHOICE or ? for help: (l/2/3/4/5/6/7/8/?)

Type **8 <enter>.**

14. Once the system has shutdown, and the >>> prompt has returned, power off the Alpha processor and disconnect the CD-ROM drive from the Alpha processor.

15. Power the Alpha processor backup.

16. Verify the Alpha processor boots correctly and start calls processing.

17. Disconnect the CRT cable from the back of the Alpha processor.

11.3.4 Crypto Change-out and Rekey Procedures (KG-94/94A)

Table 11-6 provides procedures for crypto change-out and rekey.

Table 11-6. Crypto Change-out and Rekey Procedures

STEP	ACTION
1	All sites must identify the primary office responsible for coordinating crypto change-outs (and other crypto maintenance actions) for each DRSN link terminating at their location. **Provide the Scott RNOSC with the following information:** a. Names of primary and alternate POCs b. Office telephone numbers, commercial, DSN, and secure c. E-mail address d. Duty hours e. List of links by CCSDs for which they serve as the primary office for coordinating change-outs f. List of links by CCSDs for which they serve as the secondary office for coordinating change-outs
2	One day before the change-out, coordinate with distant-end site and confirm a preferred and alternate time for initiating change-out.
3	Contact the Scott RNOSC to report completion of coordination with the distant-end site and identify the preferred and alternate times proposed for the change-out.
4	Thirty minutes before the change-out, contact and reconfirm preparations for the change-out with the distant-end site, inform the Scott RNOSC, and obtain final approval for executing the change-out.
5	Notify the Scott RNOSC on completion of the change-out and receive verification of satisfactory link operations. Support troubleshooting, as needed, to restore service if problems exist.
6	The Scott RNOSC will evaluate the preferred and alternate change-out times for potential impact on network service, based on current network conditions, and provide the preliminary approval of the preferred or an acceptable alternate change-out time. When contacted 30 minutes before the change-out, the Scott RNOSC will reassess the potential impact on network service and provide final approval on the change-out time. After receiving notification on change-out completion, the Scott RNOSC will confirm the recovery of network service or assist sites with any troubleshooting needed to satisfactorily restore service.
7	Contact the Scott RNOSC if you need additional information.

Table 11-7. Updating the KG-94/94A TEK Through Change Key Operation

STEP	ACTION
1	Before updating, check that the necessary lights are on. The POWER ON, RESYNC ACHIEVED, and FULL OPERATE lights should be lit.
2	Turn the FUNCTION SELECT switch from the LAMP TEST position to the ALARM CHECK position and momentarily depress the ACTUATE button. The ALARM light will go on briefly if the checks are satisfactory. If the ALARM light does not go on, perform a LAMP TEST. If the test is not successful, replace the KG-94/94A. If the test is successful, repeat the ALARM CHECK. If the light still does not go on, replace the KG-94/94A.
3	Turn the FUNCTION SELECT switch to CHANGE KEY and momentarily depress the ACTUATE button. The POWER ON light should be on. The OLD KEY light should go on briefly. The RESYNC ACHIEVED light will go out briefly and then stay on. ***Note:*** Updates are limited to 45 for each seed TEK.
4	On completion of the CHANGE KEY operation, check the necessary front panel lights. The POWER ON, RESYNC ACHIEVED, and FULL OPERATE lights should be lit. The update counter should advance one digit.
5	Return the FUNCTION SELECT switch to the LAMP TEST position.
6	If the above steps were unsuccessful, only the POWER ON and OLD KEY lights should be on and the update counter should not have advanced. The following steps should be taken: • The initiator of the CHANGE KEY operation should turn his FUNCTION SELECT switch from the LAMP TEST position to RESTART and momentarily depress the ACTUATE button. Only the POWER ON and OLD KEY lights should be on. • After completion of the above step, the user of the other KG-94/94A should turn his FUNCTION SELECT switch to RESTART and momentarily depress the ACTUATE button. The link should now be restored using the old TEK. The POWER ON, RESYNC ACHIEVED, and OLD KEY lights should be on. • Repeat the updating procedures. If this fails, replace the KG-94/94A at both ends of the link.
Changing the Seed TEK of an Operational Link	
1	Obtain a properly filled KYK-13, KYX-15, or KOI-18 and appropriate keying tape. ***Note:*** Both ends of the link MUST be using the same seed TEK. Check this need through orderwire.
2	Both operators should attach a fill device to their respective KG-94/94As. Use fill cable with the KOI-18 or KYX-15.
3	If using the KYK-13 or KYX-15, set the mode switch to ON/LOAD.
4	Set the ADDRESS SELECTION switch to the proper location on the KYK-13 or the KYX-15.
5	Both operators should move the KG-94/94A FUNCTION SELECT switch to LOAD and momentarily depress the ACTUATE button. The KG-94/94A PARITY light should go on.
6	If either the KYK-13 or the KYX-15 is used to key the KG-94/94A, move the KYK-13/KYX-15 MODE switch to OFF/CHECK and remove the fill device from the KG-94/94A. Proceed to step 9.
7	If using the KOI-18, insert the tape leader into the slot marked IN and line up the small holes with the white dots. Hold the ACTUATE button down and pull tape through the KOI-18 at a steady rate. ***Note:*** The use of the KOI-18 to key the KG-94/94A may need two people.
8	Release the ACTUATE button and remove the KOI-18 and fill cable from the KG-94/94A. The green PARITY light should go on.

Table 11-7. Updating the KG-94/94A TEK Through Change Key Operation (continued)

STEP	ACTION
9	Through orderwire, verify that the seed TEK has been loaded at both ends of the link, and establish which user will initiate the CHANGE KEY operation (it can be done at either end of the link, but only one needs to initiate it).
10	Both operators should check their front panel lights. The POWER ON, RESYNC ACHIEVED, and PARITY lights should be on. (If a second time through, the OLD KEY light should be on.)
11	Turn the FUNCTION SELECT switch to the ALARM CHECK position and momentarily depress the ACTUATE button. The ALARM light should go on briefly if the checks are satisfactory. If the ALARM light stays on, repeat the ALARM CHECK. After the test, if the light stays on, replace the KG-94/94A. Any other KG-94/94As involved should select CHANGE KEY by orderwire.
12	Initiator should turn FUNCTION SELECT switch to CHANGE KEY and momentarily depress the ACTUATE button. The POWER ON and PARITY lights should stay on, the OLD KEY light will flash once, and the RESYNC ACHIEVED light will go out momentarily.
13	On completion of the CHANGE KEY procedure, check the front panel lights on the KG-94/94A. The POWER ON, RESYNC ACHIEVED, and FULL OPERATE lights should be on. The update counter should reset to zero.
14	Return the FUNCTION SELECT switch to the LAMP TEST position.
15	If the above procedure was not successful, the initiator should turn the FUNCTION SELECT switch to RESTART and momentarily depress the ACTUATE button. Only the POWER ON, PARITY, and OLD KEY lights should be on. Confirm this step by orderwire.
16	The other KG-94/94A operator should turn his FUNCTION SELECT switch to RESTART and momentarily depress the ACTUATE button. The link is now restored with the old TEK. The POWER ON, RESYNC ACHIEVED, PARITY, and OLD KEY lights should be on.
17	Reload the seed TEK as above.
18	If this procedure is still not successful, replace the KG-94/94As at both ends of the link.

11.3.5 Key Management Procedures (KIV-7/HS)

Tables 11-8 through 11-12 provide procedures for KIV-7/HS key management.

Before loading keying material (KEYMAT), ensure you have the correct KEYMAT to be used. Always coordinate all key management issues with the distant-end through orderwire. Before proceeding, ensure the fill device KYK-13, KYX-15, or KOI-18 is functioning properly. If, during the procedures, you suspect the fill device to be malfunctioning or battery replacement is needed, contact the local Secure Communications Maintenance work center for assistance.

Table 11-8. Procedures to Load KEYMAT into the KIV-7/HS

STEP	ACTION
1	Coordinate and verify with the distant-end the KEYMAT being used.
2	The KIV-7 must be in the off-line condition. Observe that the ONLINE LED is extinguished.
3	Connect the fill device (KYK-13 or KOI-18) to the KIV-7. Turn on the device if using a KYK-13.
4	On the KYK-13, select the key to be transferred. If using a KOI-18, insert the tape into the KOI-18.
5	Press the **SCROLL DOWN** button twice until **[-LOAD]** is displayed.
LOADING U VARIABLE	
6	Press the **INITIATE** button; **[=LD U]** will be displayed.
7	Press the **INITIATE** button again to perform the transfer. If using a KOI-18, pull the tape through the tape reader. Observe that the **PARITY** LED on the KIV-7 flashes. If successful, the KIV-7 will display [**LOADGOOD].** If **[LOADFAIL]** is displayed, repeat steps 3 through 7.
LOADING X VARIABLE	
8	Press the **SCROLL DOWN** button twice until **[=LD X01]** is displayed.
9	Press the **INITIATE** button to perform the transfer. If using a KOI-18, pull the tape through the tape reader. Observe that the **PARITY** LED on the KIV-7 flashes. If successful, the KIV-7 will display **[LOADGOOD].** If **[LOADFAIL]** is displayed, repeat steps 3 through 9.
10	Press the **SCROLL UP** button three times until **[=Return]** is displayed.
11	Press the **INITIATE** button; **[-LOAD]** will be displayed.
12	Press the **ONLINE** button. **FDX TR** should be displayed, and the ONLINE LED should be illuminated.
Note: There are storage locations for up to ten encryption Keys for multinet application or for transmit rekey application. These locations are in the **[=LD X01]** to **[=LD X10].** Care must be taken to avoid loading a new Key over an existing Key in a storage location. The normal location for transmit rekey is **[=LD X02].**	

Table 11-9. Procedures to Update Keys in the KIV-7/HS

STEP	ACTION
1	Coordinate with the distant-end when updating keys.
2	The KIV-7 must be in the off-line condition. Observe that the ONLINE LED is extinguished.
3	Press the **SCROLL DOWN** button until **[-VU/cnt]** is displayed and press **INITIATE**.
4	Press the **SCROLL DOWN** button to the Key location needing the update. Example: **[=X01:001]**, where 001 is the current update count.
5	To update the location, press **INITIATE.**
6	Press the **SCROLL DOWN** button until **[° CONFIRM]** is displayed and press **INITIATE.**
7	Observe the count. Using the example in step 4, display should read **[=X01:002].**
8	Repeat steps 5 through 7 to update the same Key again.
9	Press the **SCROLL UP** button until **[=Return]** is displayed and press **INITIATE**. This action will exit the submenu.
10	Press the **ONLINE** button. **FDX TR** should be displayed, and the ONLINE LED should be illuminated.

Table 11-10. Procedures to TX a Key Stored in the KIV-7/HS to Distant-End

STEP	ACTION
1	The KIV-7 must be on-line and in sync with the distant-end.
2	Press the **SCROLL DOWN** button until **[-TXrekey]** is displayed and press **INITIATE.**
3	Press the **SCROLL DOWN** button until the fill location of the Key to be transmitted is displayed. Example: the current operational Key is in location 01, location to be transmitted is location 02. Scroll until **[=Snd X02]** is displayed.
4	Press the **INITIATE** button.
5	Observe the display. Rekeying should be displayed momentarily, then **[Snd Good]** should be displayed. If **[Snd Fail]** is displayed, repeat these steps and ensure the KIV-7 is in synchronization with the distant-end.
6	When the rekey operation is completed, the KIV-7 will attempt to regain synchronization with the distant-end in the current operational Key location. Using the example in step 3, that would be location 01, **NOT** the Key transmitted in location 02.
7	To regain synchronization with the distant-end, use the Key select steps in Table 11-12. Using the example in step 3, you would use the steps in Table 11-12 to select Key location 02.

Table 11-11. Procedures to Zeroize Keys in the KIV-7/HS

STEP	ACTION
1	The KIV-7 can be in the on-line or off-line state.
2	Simultaneously press the **INITIATE** and **ZEROIZE** buttons.
3	Observe that the PARITY and ALARM LEDs are illuminated.

Table 11-12. Procedures to Select a Key for Operation in the KIV-7/HS

STEP	ACTION
1	The KIV-7 can be in the on-line or off-line state.
2	Press the **SCROLL DOWN** button until **[-SEL KEY]** is displayed and press **INITIATE.**
3	Press the **SCROLL DOWN** button to the Key location to be used. The operational Key selected will be highlighted.
4	Press the **INITIATE** button.
5	Observe the message display and the **PARITY** LED. If the selected location is not loaded or valid, the KIV-7 will go off-line and the **PARITY** LED will remain illuminated. If the selected location is loaded and valid and the KIV-7 is in the on-line mode, the KIV-7 will attempt to resynchronize with the distant-end. If the KIV-7 is in the off-line mode, reinitiate synchronization by pressing the **ONLINE** button.
6	Press the **SCROLL DOWN** button until **[Return]** is displayed. Press **INITIATE** to exit the submenu.

SECTION 12
LOGISTICS AND REPAIR PARTS SUPPORT

12.1 PURPOSE

This section identifies procedures for O&M day-to-day logistics and repair parts support for DRSN switching, transmission, and associated equipment.

12.2 SECTION CONTENTS

The topics covered in this section are IDNX/Promina and RED switch logistics support.

12.3 INTEGRATED DIGITAL NETWORK EXCHANGE LOGISTICS

The IDNX/Promina equipment installed in the DRSN is commercial-off-the-shelf (COTS) equipment and is not logistically supportable through existing supply channels. Therefore, on a day-to-day basis, most of the maintenance actions needed by site personnel involve initially isolating the source of the problem and taking those steps needed to physically replace the faulty component once the new component is received on-site. The basic procedures are found in Table 12-1.

12.4 DRSN RED SWITCH LOGISTICS

A framework for DRSN RED switch logistics support is provided in the *Joint Logistic Support Plan (SP*) dated 13 July, 1998. The DRSN is comprised primarily of COTS equipment that is supported by contractors. Coordination and management of the initial spare parts inventory is the responsibility of the individual sites. The paragraph 6.3 of the SP provides detailed procedures regarding spares and repair part support for all DRSN switching equipment.

Table 12-1. IDNX/Promina Logistics

IDNX/ Promina	LOGISTICS SUPPORT PROCEDURES
1	Once it has been determined that an IDNX/Promina component is faulty and needs to be replaced, contact the appropriate RNOSC. Usually, fault isolation will be accomplished with support from the RNOSC. **Note:** The operations centers are manned 24-hours-per-day, 7-days-per-week.
2	Provide the RNOSC with the following information needed to ensure the replacement parts are properly shipped: • Location and affected node number • Major end item and faulty component it is a part of • Card type, part name, or other identifying numbers • Revision number, if applicable • Quantity needed • Complete mailing or shipping address to include - Organization and office symbol - Building and room number - Base name or location with the zip code - POC (name and commercial number) for shipment

SECTION 13
DRSN MANAGEMENT DATABASE SYSTEM

The following template is the information requested by the DISA Program Management Office (PMO) to ensure all feasible points of contact needed to support the DRSN in any contingency are available for managers at HQ DISA and the RNOSCs. We solicit your assistance in providing this information and in keeping our O&M database current. The complete database will be maintained by the PMO at DISA HQ, and provided to the RNOSCs as it is updated. Your office will be contacted periodically to determine if any changes or updates need to be made. We do not expect every position to be filled and are aware that in many cases one person may cover several positions. Please provide as much information as possible and inform us of any additional names, positions or responsible parties you think would be useful. Your assistance will help us provide system and network updates and policies to you in the field as rapidly as possible and prevent surprises that happen when key people do not get included in correspondence. Please complete the information and forward by fax or mail to:

DISA/NS54
11440 Isaac Newton Square
Reston, VA 20190-5006

Commercial: (703) 735-8033 or DSN (312) 653-8033
Fax: (703) 735-8980 or DSN (312) 653-8980

Switch POC Listing

Command: _____ **R-Code** _____ **Type:** _____

Location: _____ **Theater:** _____ **MILDEP:** _____

CINC Communications Support: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title: _____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: _____ *** Alternate Contact (Name and DSN #):** _____

Circuit Control Office:

Mailing Address:

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____

Title: _____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: _____ *** Alternate Contact (Name and DSN #):** _____

Job Control: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title: _____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: _____ *** Alternate Contact (Name and DSN #):** _____

FOR OFFICIAL USE ONLY

Crypto Maintenance: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title: _____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: _____ *** Alternate Contact (Name and DSN #):** _____

DRSN Management: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title: _____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: _____ *** Alternate Contact (Name and DSN #):** _____

DRSN Maintenance: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title: _____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: _____ *** Alternate Contact (Name and DSN #):** _____

DRSN COR: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title: _____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: _____ *** Alternate Contact (Name and DSN #):** _____

FOR OFFICIAL USE ONLY

DRSN O&M Support: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title: _____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: _____ *** Alternate Contact (Name and DSN #):** _____

DRSN QAE: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title: _____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: _____ *** Alternate Contact (Name and DSN #):** _____

DRSN Site Coordinator: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title: _____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: _____ *** Alternate Contact (Name and DSN #):** _____

DRSN CCB Representative: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title: _____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: _____ *** Alternate Contact (Name and DSN #):** _____

FOR OFFICIAL USE ONLY

CCSS Product CCB Representative: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title:_____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: ___ _____ *** Alternate Contact (Name and DSN #):** _____

ISSO: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title:_____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: ___ _____ *** Alternate Contact (Name and DSN #):** _____

ISSM: **Mailing Address:**

Name: _____ **DSN Phone #:** _____ **Non-Secure FAX #:** _____ _____

Rank: _____ **CMRL Phone #:** _____ **Secure FAX #:** _____ _____

Title:_____ **DRSN Phone #:** _____ **PLA:**

_____

E-mail: ___ _____ *** Alternate Contact (Name and DSN #):** _____

FOR OFFICIAL USE ONLY

Intentionally left blank

SECTION 14
ACRONYMS AND ABBREVIATIONS

2-W	Two-Wire
4-W	Four-Wire
497 IG	497th Intelligence Group
A/O	Authorized Outage
AAF	Army Air Field
AB	Air Base
ACC	Air Combat Command
AETC/CC	Air Education and Training Command/Command Center
AF	Air Force
AFB	Air Force Base
AFIC-AIA	Air Force Intelligence Command-Air Intelligence Agency
AFMC	Air Force Material Command
AFSOC	Air Force Special Operations Command
ALT SOUTH	Southern Command Alternate Location
AM	Accounting Management
AMC	Air Mobility Command
ANDVT	Advanced Narrowband Digital Voice Terminal
ANMCC	Alternate NMCC
ANSI	American National Standards Institute
APROC	"A" Processor
ARDIMSS	Advanced DRSN Integrated Management Support System
ASCII	American Standard Code for Information Interchange
AU/CC	Air University/Command Center
AUTODIN	Automatic Digital Network
b/s	Bits Per Second
BBS	Bulletin Board System
BE	Belgium
BPROC	"B" Processor
CC	Command Center
CCSD	Command Communications Service Designator
CDH	Call Detail History
CDS	Clock Distribution System
CINC	Commander in Chief
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CLK	Clock
CM	Configuration Management
CMC	Commandant Marine Corps
COMSEC	Communications Security
COTS	Commercial-off-the-Shelf
CP	Camp

CRT	Cathode Ray Tube
CSO	Communications Support Officer
CSU	Channel Service Unit
CWD	Communications Watch Division
DA II	Dual Analog II
DAA	Designated Approving Authority
DAT	Digital Audio Tape
DCI	Direct Crypto Interface
DCID	Director of Central Intelligence Directive
DCO	Dial Central Office
DCL	Direct Communications Link
DCS	Defense Communications System
DEC	Digital Equipment Corporation
DIA	Defense Intelligence Agency
DIGVAL	Digital Validation Table
DII	Defense Information Infrastructure
DISAC	DISA Circular
DISN	Defense Information Systems Network
DODD	DOD Directive
DOS	Disk Operating System
DPA	Dual Phone Adapter
DPM	Digital Phone Multiplexer
DRSN	Defense RED Switch Network
DSA	Digital Speaker Assembly
DSN	Defense Switched Network
DSS	Digital Small Switch
DSS-1	Digital Small Switch-1
DTA	Dual Trunk Adapter
DTMF	Dual-Tone Multifrequency
EBBS	Electronic Bulletin Board System
ECP	Engineering Change Proposal
EPC	Early Pentagon Capability
ESC	Executive Support Center
EUCOM	European Command
EUR	Europe
F.O.	Fiber Optic
FCO	Facility Control Office
FM	Fault Management
FORSCOM	Forces Command
FOUO	For Official Use Only
FT1	Fractional T1
FTP	File Transfer Protocol
FTS	Federal Telecommunications System

FTS2000	Federal Telecommunications System 2000
FY	Fiscal Year
GE	Germany
GNOSC	Global Network Operations and Security Center
GPS	Global Positioning System
HAZCON	Hazardous Condition
HF	High Frequency
HQ	Headquarters
IAW	In Accordance With
ID	Identification
IDNX	Integrated Digital Network Exchange
IP	Internet Protocol
ISSM	Info System Security Manager
ISSO	Information System Security Officer
IST	Integrated Services Telephone
IT	Italy
J6T	Joint Staff
JCS	Joint Chiefs of Staff
JIEO	Joint Interoperability and Engineering Organization
kb/s	Kilobits per Second
KEYMAT	Keying Material
KG	Key Generator
kHz	Kilohertz
KMC	Key Management Center
KPI	KG Phone Interface
KTI	KG Trunk Interface
LAN	Local Area Network
LBCI	Loss of Bit Count Integrity
LBT1	Limited Bandwidth T1
LCC	Low Cost Command Console
LED	Light Emitting Diode
MAJCOM	Major Command
Mb/s	Megabits per second
MHz	Megahertz
MILDEP	Military Department
MTF	Message Text Format
N/A	Not Applicable
NAS	Naval Air Station

NATO	North Atlantic Treaty Organization
NCA	National Command Authorities
NCO	Network Control Office
NCSA	National Center for Super Computing Applications
N.E.T.	Network Equipment Technologies, Inc.
NM	Network Management
NMCC	National Military Command Center
NMS	Network Management Subsystem
NORAD	North American Air Defense Command
NSA	National Security Agency
O&M	Operations and Maintenance
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OO-ALC	Odgen AFB - Air Logistic Center
PAC	Pacific
PACAF	Pacific Air Force
PACOM	Pacific Command
PC	Personal Computer
PCS	Permanent Change of Status
PM	Performance Management
POC	Point of Contact
POTS	Plain Old Telephone Service
PRC	Primary Rate Card
PSCS	Pentagon Secure Conference System
PSN	Public Switched Network
PTF	Patch and Test Facility
PWA	Printed Wiring Assembly
QAS	Quad Asynchronous
QASD	Quad Asynchronous Data
QTI	Quad Telephone Interface
RCSSII	Rack, Cardcage, Slot, and Interface Number
RFO	Reason for Outage
RFS	Request for Service
RNOSC	Regional Network Operations and Security Center
ROUVAL	Route Validation
RSU-1	Electrospace 240-port Digital Switch
SAL	Security Access Level
SALVAL	Security Access Level Validation
SATCOM	Satellite Communications
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility

SDN	Subscriber Directory Number
SDS	Secure Digital Switch
SDS-1	Raytheon 1600-Port Digital Switch
SHAPE	Supreme Headquarters Allied Powers Europe
SM	Security Management
SP	Joint Logistics Support Plan
SSO	Special Security Officer
STI	Summing Telephone Interface
STRATCOM	Strategic Command
STU-II	Secure Telephone Unit, Second Generation (KY-71)
STU-III	Secure Telephone Unit, Third Generation
STU-III/R	Secure Telephone Unit, Third Generation/Remote
SYSOP	System Operator
T&S	Timing and Synchronization
TBD	To Be Determined
TCF	Technical Control Facility
TCO	Telecommunications Certification Office
TCP	Transmission Control Protocol
TEK	Traffic Encryption Key
TFW	Tactical Fighter Wing
TRANSCOM	Transportation Command
TRI-TAC	Tri-Services Tactical Communications
TRK	Trunk
TSO	Telecommunications Service Order
TSR	Telecommunications Service Request
TX	Transmit
UHF	Ultra High Frequency
UIC	User Identification Code
UK	United Kingdom
URL	Uniform Resource Locator
US/FORN	United States/Foreign
USACOM	U.S. Atlantic Command
USAFE	U.S. Air Forces-Europe
USAREUR	U.S. Army-Europe
USCENTCOM	U.S. Central Command
USD	Universal Synchronous Data
USFK	U.S. Forces, Korea
USMC	U.S. Marine Corps
USNAVCENT	U. S. Naval Forces Central Command
USNAVEUR	U.S. Navy, Europe
USPACOM	U.S. Pacific Command
USSOCOM	U.S. Special Operations Command
USSOUTHCOM	U.S. Southern Command
USSPACECOM	U.S. Space Command

USSTRATCOM	U.S. Strategic Command
VDC	Volts Direct Current
WHCA	White House Communications Agency
WWSVCS	Worldwide Secure Voice Conferencing System
WWW	World Wide Web